Departamento de Polícia Federal – DPF

Associação Nacional dos Peritos Criminais Federais – APCF

ICCyber'2004

Anais da 1ª Conferência Internacional de Perícias em Crimes Cibernéticos

Proceedings of the 1st International Conference on Cyber Crime Investigation

Anales de la 1ª Conferencia Internacional de Investigación sobre Delitos Cibernéticos

Setembro 2004

Editora DPF
Departamento de Polícia Federal

Proceedings of the 1st International Conference on Cyber Crime Investigation (ICCyber'2004) / Departamento de Polícia Federal (ed.) – Brasília, Brazil, 2004, 238 pp. – ISBN 85-98547-01-8

ISBN 85-98547-01-8

PREFÁCIO

O uso da Internet vem crescendo muito rapidamente, inclusive para uso de aplicações comerciais envolvendo grandes quantidades de valores financeiros nas incontáveis transações comerciais realizadas a todo instante. Lembre-se que não há fronteiras que possam limitar essas transações e todos os contatos feitos por meio do espaço cibernético. Este ambiente se tornou extremamente propício para o surgimento e o crescimento dos chamados crimes cibernéticos, principalmente devido à possibilidade do anonimato de seus usuários, à facilidade de uso da grande rede e à sua conexão com todo o mundo.

Dessa forma, para que o combate a esses crimes possa ser eficaz e também eficiente, principalmente quando são praticados ou têm efeitos em vários países, mister se faz a cooperação internacional por meio de instituições organizadas e estruturadas para esse fim. Além disso, é importante fomentar a pesquisa e o desenvolvimento no âmbito da perícia de informática. Com esses objetivos, sob os auspícios do Departamento de Polícia Federal, a Diretoria Técnico-Científica e o Instituto Nacional de Criminalística, por meio do Serviço de Perícias em Informática (SEPINF), estão promovendo a ICCyber'2004 – I Conferência Internacional de Perícias em Crimes Cibernéticos. A pretensão é que a conferência seja realizada periodicamente de dois em dois anos.

A idéia de realizarmos uma conferência internacional de perícias em crimes cibernéticos surgiu da necessidade de promovermos discussões científicas, em nível mundial, relativas às questões técnico-científicas e jurídicas referentes aos crimes cibernéticos, de modo a fomentar a pesquisa e o desenvolvimento visando ao combate aos crimes cibernéticos, com a participação efetiva dos peritos criminais federais de informática e dos demais policiais brasileiros e estrangeiros, promovendo-se uma aproximação maior com outras comunidades da computação com atuação na área forense.

Outro fato que motivou o surgimento deste evento é a necessidade de estreitarmos o nosso relacionamento com a comunidade científica internacional da área, bem como com organismos internacionais, como a "Rede 24/7" e a Interpol, dentre outros, no sentido de implantarmos um sistema ágil de cooperação policial internacional visando ao combate dos crimes cibernéticos, principalmente daqueles que têm efeitos em vários países.

A ICCyber´2004 tem como foco principal incentivar a pesquisa e o desenvolvimento científicos, com o objetivo de se produzirem técnicas novas e avançadas, visando ao combate aos crimes cibernéticos. O programa científico desta Conferência está estruturado em sessões técnicas, organizadas por Peritos Criminais Federais da área de Informática, podendo receber artigos convidados e artigos regulares selecionados pela Comissão Técnica de Avaliação.

A ICCyber'2004 tem papel de fundamental importância, visto que, por meio desse evento, estarão sendo incentivadas as atividades de pesquisa e de desenvolvimento científicos na área de perícia de informática. Também estarão sendo possibilitados os intercâmbios técnicos e científicos entre os peritos criminais federais e outros profissionais brasileiros e estrangeiros envolvidos em atividades correlatas, como outros peritos e investigadores, cientistas da computação e juristas atuantes nessa área, dentre outros.

Geraldo Bertolo
Diretor Técnico-Científico

REALIZAÇÃO

Presidente da Conferência
PAULO FERNANDO DA COSTA LACERDA
Diretor-Geral do DPF

Vice-Presidente da Conferência
GERALDO BERTOLO
Diretor Técnico-Científico

Coordenador da Conferência
OCTÁVIO BRANDÃO CALDAS NETTO
Diretor do Instituto Nacional de Criminalística

COMITÊ ORGANIZADOR

PAULO QUINTILIANO DA SILVA
Chefe do Serviço de Perícias em Informática

RAFAEL PINTO COSTA
Perito Criminal Federal

MARCELO CALDEIRA RUBACK
Perito Criminal Federal

MARCOS AURÉLIO MENDES DE MOURA
Perito Criminal Federal

ROOSEVELT A. F. LEADEBAL JR
Presidente da APCF

SECRETARIA

APCF – Associação Nacional dos Peritos Criminais Federais
CENTRO EXECUTIVO SABIN - SEPS 714/914 – Salas 223/224
Brasília DF: 70.390-145 Fone: +55 (61) 0800 703 2723

TEMAS DAS SESSÕES

Tema I - Legislação aplicada aos crimes cibernéticos

01 - Legislação aplicada aos crimes cibernéticos

Tema II - SPAM/SCAM contra entidades financeiras

02 - SPAM/SCAM contra entidades financeiras

Tema III – Crimes no Espaço Cibernético

03 - Terrorismo Cibernético

04 - Crimes praticados no Espaço Cibernético.

05 - Perícia em Locais de Crimes de Divulgação de Informações criminosas por meio da Internet.

Tema IV – Perícia Criminal em Informática

06 - Perícias em Computadores.

07 - Perícias em Sistemas de Informações Automatizados

08 - Perícias em Mídias de Armazenamento Computacional.

09 - Extração de dados em equipamentos eletrônicos programáveis.

10 - Perícias em Agendas Eletrônicas.

11 - Perícias em Aparelhos Celulares.

12 - Perícias em Máquinas Caça-Níqueis.

13 - Ferramentas Periciais aplicadas à investigação de crimes cibernéticos

Tema V – Tecnologias correlatas

14 - Prevenção e Detecção de Intrusão.

15 – Biometria

16 - Segurança em Redes de Computadores.

17 - Criptologia.

18 - Aplicações forenses para o combate aos Crimes Cibernéticos.

19 - Processamento e Tratamento de Imagens Digitais.

20 - Reconhecimento de Padrões.

SESSÕES PLENÁRIAS

- ***Sessão Plenária I: E-crime in Australia - a Law Enforcement Response***

  The origins of high tech crime investigations
  Nigel Phair, Australian Federal Police, Australia

- ***Sessão Plenária II: Legislação brasileira sobre crimes cibernéticos***

  Legislação brasileira sobre crimes cibernéticos
  Luiz Piauhylino, Deputado Federal, Brasil

  Legislação brasileira sobre crimes cibernéticos
  Marcos Abramo, Deputado Federal, Brasil

- ***Sessão Plenária III: Crimes Cibernéticos no âmbito Internacional***

  Interpol's Role in Combating International Cybercrime
  Marc Goodman, Interpol, USA

  Mitos y Realidades de Virus y Antivirus y su Influencia en el Fraude Cibernetico
  Carlos Lang, Colaborador Del Grupo de Delitos Cibernéticos de la Policia Federal Preventiva, Mexico

  Situacion del Delito Informatico en España
  Jose Antonio Lozano Gonzalez, Guardia Civil, España

- ***Sessão Plenária IV: Legislação internacional sobre crimes cibernéticos***

  International legislation about cybercrime
  Todd Hinen, Department of Justice, USA

  Breaking Digital Evidence in Court
  Boaz Guttman, National Privacy Concil, Israel

- ***Sessão Plenária V: Investigação de crimes cibernéticos no contexto internacional***

  The International Threat from Serious and Organised Crime
  Len Hynds, Head of The National Hi-Tech Crime Unit, UK

  Hunting Hackers: An Overview of the U.S. Army Criminal Investigation Command (CID)
  Daniel T. Andrews, Computer Crime Investigative Unit, US Army, USA

- ***Sessão Plenária VI: Pornografia Infantil na Internet***

  Trafficking and Child Pornography
  Zackery Lowe, Supervisory Special Agent, FBI, USA

  Investigación de Delitos de Pornografia Infantil por Internet
  Luis Garcia Pascual, Inspector del Corpo Nacional de Policia, Brigada de Investigación de Delitos Tecnologicos, España.

- ***Sessão Plenária VII: Tecnologias Correlatas***

  Analysis & Forensics for Physical e Cyber Security Systems
  Paulo R. Prado, Computer Associates

  Avaliação do Software e-Trust
  Sérgio Luís Fava, Rafael Pinto Costa
  Polícia Federal, Brasil

  Reconhecimento Facial Aplicado à Perícia Criminal
  Paulo Quintiliano da Silva, Polícia Federal, Brasil

- ***Sessão Plenária VIII: Segurança nas Transações Eletrônicas***

  eBay-Mercado Libre – Trust and Safety Program
  Marco Aurélio Brasil Lima, eBay – Mercado Libre, USA

PALESTRAS DAS SESSÕES PLENÁRIAS - INFORMAÇÕES

Legislação brasileira sobre crimes cibernéticos
Deputado Marcos Abramo

- Falha no ordenamento jurídico vigente, com relação ao combate à crimes de informática.
- Aperfeiçoamento de projetos para edição de normas que regulamentem o acesso mundial de computadores, afim de coibir práticas de atos criminosos, visando adequação da legislação brasileira à Convenção de Crimes Cibernéticos do Conselho da Europa.
- Abordagem do Projeto de Lei de n.º 3301/04 que tem por objetivo definir responsabilidades para os provedores de acesso, criar regras para o registro de usuários da Internet, definindo assim, uma nova política de segurança que regulamentará as atividades dos provedores.

Resumo

A criminalidade informática é uma manifestação da atualidade, que deve ser combatida. A discussão deve centrar em torno das modalidades técnicas de previsão, em referência à dúvida de se abrir caminho a uma legislação especial e autônoma, ou então a medidas que inserissem as disposições incriminadoras no corpo do Código Penal de 1940, ora vigente.

Não temos dúvida de que a Internet é um meio novo de praticar velhos crimes, entretanto esses crimes não são considerados "Crimes de Informática". Estelionato, por exemplo, é sempre estelionato, praticado com ou sem a assistência do computador; afirmar que alguém cometeu um fato definido como crime, sem que tal seja verdade, configura delito de calúnia (CP, art 138), tanto quando a difusão é feita oralmente ou pelos caminhos da Internet.

No entanto, não se deve confundir um crime comum praticado pelo uso ou contra o computador de um "Crime de Informática" propriamente dito. Por isso é que defendo uma legislação específica acerca desses comportamentos novos, os "Crimes de Informática", até então desconhecidos pelo legislador pátrio de 1940, surgidos com o advento do computador e da Internet.

Devemos ter em mente, que não é pelo fato de alguns qualificarem o espaço cibernético como um novo mundo ou mundo virtual, que existam dois universos diferentes – um real e outro imaginário – vez que, na verdade, há apenas um, onde todos nós vivemos, e no qual se precisa aplicar e observar os mesmos valores de liberdade, dignidade e respeito aos direitos do semelhante.

Interpol's Role in Combating International Cybercrime
MARC GOODMAN, Sênior Advisor, USA

Over 75 years ago, Interpol was chartered by 14 nations to deal with mounting levels of transnational crime. Today Interpol's membership has grown to 181 nations, reflecting not only the seriousness of the criminal threat, but also the desire of all peoples around the world to live in peace and security. As the world's only global policing organization, Interpol is dedicated to making the world a safer place in which to live.

Given the global nature of today's financial and telecommunication networks, the majority of computer crimes are international both in their scope and reach. In that respect, Interpol is perfectly situated to play a significant role in combating the international dimensions of high technology crime. For over a decade, Interpol has actively been involved in combating high tech crime. Rather than 're-inventing the wheel', the Interpol General Secretariat has harnessed the expertise of its members in the field of cybercrime through the vehicle of a 'working party' or a group of experts. Interpol brings together the expertise of its members in the field of cybercrime by means of regional working parties for E urope, Asia, the Americas and Africa.

The goal of these working parties is to set technical standards, share criminal intelligence, train law enforcement personnel, and facilitate cybercrime investigations around the world. All working parties are in different stages of development. It should be noted that the work done by the working parties is not Interpol's only contribution to combating ITC, but it certainly represents the most noteworthy contribution to date.

Breaking Digital Evidence in Court
BOAZ GUTTMAN, National Privacy Concil, Israel

Background

On 13 June 2002 an indictment was served by the State Attorney for the Haifa District, Ms. Lily Burishansky, against Mr. Michael Lerman, born in 1962, for obstructing computer material, penetrating into computer hardware, and disseminating a virus, offences under Sections 2 + 4 + 6 of the 1995 Computer Law, as well as for intrusion of privacy, an offence under Section 5 of the 1981 Protection of Privacy Law.

Prior to his ultimate job, private investigator Michael Lerman, aged 42, was a member of an undercover unit of the Israeli police - a secret unit specializing in surveillance of suspects.

The indictment was published in the Israeli press before the accused was informed about it. The trial, which opened in court on 21 November 2002, has not yet ended. The case is being heard by Justice Kamal Sa'ad who is currently the Registrar of the District Court. In December 2003, a witness for the prosecution died – Mr. Nasser Salameh, who was a member of the police unit for computer crimes. Salameh did not give evidence in the trial.

The judge decided to accept as evidence all the digital correspondence that Salameh had edited, processed, and printed. During the trial, it transpired that Superintendent Eyal Peterburg - a senior police officer and investigator of computer crimes – had made a new, later copy from the hard disk in Lerman's computer, which was seized by Salameh in May 2001; Detective Peterburg did not make use with the copy of the computer made by Nasser Salameh.

Following is an excerpt from the court transcript for 21 June 2004. Cross-questioned by the defender, Detective Eyal Peterburg was asked to show the judge the names of the files appearing in the computer printouts that were submitted to the court, on the computer that was brought into the courtroom. The printouts, which were printed out and marked on 13 May 2001, show the icon of a tool used by the police, which "captures" digital evidence. The tool is a software program called *SnagIt*. While being questioned, the accused was surprised to hear that the tool had been installed on his computer. On 21 June 2004, when the police were asked to open the computer itself in the courtroom, both the tool itself and its icon were missing.

The central question is - did someone in the police change the evidence entirely and/or partially on the hard disk of the accused's computer? Alternatively – when the evidence was copied onto the hard disk that was given to the court and to the prosecution as well as the defence, was it done in a reliable way? Following is the transcript of the relevant section and a photocopy of the computer printout that already appeared in the court transcript before Detective Peterburg gave evidence.

The International Threat from Serious and Organised Crime
LEN HYNDS, Head of The National Hi-Tech Crime Unit, UK

DCS Len Hynds has served at a tactical, strategic and policy level in more than 30 countries spanning four continents, working in partnership with foreign colleagues to prosecute and disrupt international criminal networks, and to streamline investigation procedure.

He was selected as the first head of the NHTCU, with the responsibility for the development and implementation of a national centre of excellence to combat hi-tech crime and delivery of benchmark standards for all local computer crime units within England and Wales. He has advised the UK Government on proposed legislation, attended the United Nations Commission on Narcotic Drugs as advisor to the British delegation and led EU funded workshops examining the harmonisation of law enforcement effort.

He was involved in the formation of the National Crime Squad and is acknowledged as the architect of the Operational Protocol between the National Crime Squad and HM Customs and Excise. Additionally he chairs the UK Internet Crime Forum, and the Association of Chief Police Officers National Hi-Tech Crime Working Group.

Reconhecimento Facial Aplicado à Perícia Criminal
PAULO QUINTILIANO, Polícia Federal, Brasil

Neste artigo é apresentado um breve histórico do reconhecimento facial. São também abordados alguns aspectos psicológicos do assunto e modelos propostos para o entendimento da percepção facial. Um modelo de reconhecimento facial automatizado, baseado nas *eigenfaces*, é proposto e apresentado em detalhes. São apresentadas aplicações do algoritmo de reconhecimento facial para a perícia criminal, especialmente para o reconhecimento de pessoas em cenas de crimes. Com a finalidade de reconhecer pessoas com a face semi-oclusa, com o uso de máscaras ou outro artefato, normalmente em cenas de crimes, os conceitos das *eigenfaces* são estendidos para *eigeneyes, eigenmouth* e *eigennose*, com a finalidade de reconhecer as pessoas nessa situação adversa.

Mitos y Realidades de Virus y Antivirus y su Influencia en el Fraude Cibernetico
CARLOS LANG, Mexico

Son virus problema de seguridad nacional. Los virus van más allá de inhabilitar una máquina, borrar información y parar la productividad en una empresa, son un problema de seguridad nacional, advirtió Carlos Lang, colaborador del Grupo de Delito Cibernético de la Policía Federal Preventiva. Y es que de acuerdo con el especialista, un ataque informático combinado, es decir aquel que emplea virus, gusano y troyanos, es capaz de paralizar hospitales, bancos, semáforos y provocar apagones. En algunos casos, dijo, puede hasta provocar la muerte de personas, como ocurrió con un enfermo que falleció en México debido al daño causado por el virus SQL Slammer en un servidor de un hospital, y que al dañar el expediente, impidió dar la atención adecuada al paciente.

"En países como Estados Unidos se está buscando que los ataques de virus se tipifiquen como terrorismo y que los hackers sean castigados como terroristas, en México estamos reuniendo esfuerzos para combatir (los ataques informáticos)", expresó. Hay países, agregó, donde un ataque informático es declarado como alerta nacional, pues tienen que proteger al usuario. Durante su participación en el evento organizado por el Tec de Monterrey, el especialista en seguridad informática aseguró que en México existe la tecnología para rastrear ciberdelitos y detener a los hackers, sólo que a veces éstos son muy hábiles y casi siempre logran escapar.

"(En el País) tenemos una policía cibernética que se encarga de resolver los ciberdelitos y ya existen avances en cuestiones legislativas, no estamos muy avanzados, pero tampoco estamos tan atrasados", aseguró. Lang agregó que México ocupa el octavo lugar en creación de virus, en una lista encabezada por Corea del Sur, Polonia y la República Checa.

The origins of high tech crime investigations
Nigel Phair, Australian Federal Police, Australia

- why have an Australian High Tech Crime Centre?
- role and responsibilities of the AHTCC;
- whole of government approach to high tech crime;
- critical infrastructure protection;
- public/private partnership in high tech crime;
- types of investigations undertaken by the AHTCC;
- how these investigations are carried out;
- international cooperation;
- high tech crime training initiatives;
- trends and issues in high tech crime;
- future developments in high tech crime.

SESSÕES TÉCNICAS - ARTIGOS

FERRAMENTAS DE ESTEGANOGRAFIA E SEU USO NA INFOWAR

Laura Cristina Machado Coelho

Ricardo Jorba Bento

ABSTRACT

With the fast and increasing improvement of communication technology, a new battle field was formed, the Internet, where there are no concrete objectives, we don't know who really is the enemy, nor even the kind of weapons, used techniques and the extent of the damage that can be caused. Because of this, the called Infowar is most feared kind of battle nowadays. This paper will approach one of the most efficacious techniques used in Infowar: the Steganography. Such techniques consist in the covering the information in many ways like images, texts, audio and video. Steganography can be also used for illegitimate reasons, for example, steal data and send them, through an innocent e-mail. Considering all this, we tested many steganography tools with the aim to understand their operation.

1. INTRODUÇÃO

A informação é algo que leva o homem a grandes conquistas, guerras e destruição. Com o advento da internet, a troca de informações se deu de forma mais veloz e em pouco tempo se tornou o meio de comunicação mais utilizado, não só para a própria comunicação ou pesquisas escolares, mas também como meio de fornecer serviços que envolvem investimentos econômicos. A internet, inicialmente, não previa nem seu crescimento estrondoso, nem tão pouco que pudessem aparecer pessoas especializadas em roubar informações e utilizá-las como meio de terrorismo e atentados contra as nações e os seres humanos.

A guerra da informação é uma batalha que amedronta muito as grandes empresas e o próprio governo. Utilizando o roubo ou o uso indevido da informação pode-se destruir grandes negócios em poucos minutos. Os meios e os motivos podem ser a destruição ou apropriação indevida da informação por imperícia de quem a utiliza, insatisfação de funcionários, por um concorrente ou simplesmente por estrelato.

Para não serem descobertos, os chamados piratas de computador, ou hackers, passaram a inovar em suas técnicas nas trocas de informação. Hoje, uma das técnicas mais eficazes se chama: esteganografia. Tal técnica utiliza textos, imagens, sons e vídeos para esconder informações de forma que as mesmas passem desapercebidas aos olhos humanos. Acredita-se que grandes atentados terroristas como os de 11 de Setembro de 2001, tenham sido estruturados e planejados utilizando esteganografia como principal meio de comunicação.

2. ESTEGANOGRAFIA NA *INFOWAR*

A esteganografia pode ser usada por razões ilegítimas, por exemplo, roubar dados e esconder em um arquivo e emiti-los para fora por meio de um inocente e-mail. Além disso, uma pessoa, com um passatempo de salvar arquivos pornográficos, pode esconder a evidência com o uso de esteganografia. E, para finalidades terroristas, pode ser usado como meio de uma comunicação secreta.

A esteganografia é fonte de muita discussão, particularmente quando se suspeitou que terroristas, nos ataques de 11 de setembro, podem tê-la usado para comunicações secretas [26]. Enquanto nenhuma conexão for provada, o interesse indica a eficácia da esteganografia como meios de obscurecer dados. Certamente, junto com a criptografia, a esteganografia é uma das maneiras fundamentais para que dados sejam mantidos confidenciais.

3. DEFINIÇÃO DE ESTEGANOGRAFIA

Esteganografia é uma palavra de origem grega, onde *Stegano* significa escondido ou secreto e *Grafia*: escrita ou desenho.

Não se deve confundir criptografia com esteganografia, pois o primeiro esconde o conteúdo de uma mensagem e a existência desta é conhecida, já o segundo esconde a existência da mensagem. Ambas as técnicas podem ser utilizadas em conjunto para se obter um maior grau de segurança da informação.

Como muitas ferramentas de segurança, a esteganografia pode ser usada para uma variedade de razões, algumas boas, outras nem tanto. As finalidades legítimas podem incluir imagens de marca d'água por motivo de proteção de direitos autorais.

As marcas d'água digitais são similares à esteganografia no que tange à ocultação de dados, os quais parecem ser parte do arquivo original e não são facilmente detectáveis por qualquer pessoa.

Finalmente, a esteganografia pode ser usada para manter a confidencialidade da informação valiosa, para proteger os dados de possíveis sabotagens, roubo, ou apenas visualização desautorizada.

4. TERMINOLOGIA ADOTADA

A terminologia para descrever um subconjunto de informação oculta foi definida no **Information Hiding Workshop**[1]**,** realizado em Cambridge, Inglaterra em Abril de 1996.

A descrição [3] de esteganografia – "escrita oculta" – pode ser feita basicamente da seguinte forma:

> O **dado embutido** (*embedded data*) é a informação que alguém deseja enviar em segredo. Este dado geralmente fica escondido em uma mensagem aparentemente inocente, chamada de **recipiente ou de objeto cobertura** (*container* ou *cover-object*), produzindo um **estego-objeto** (*stego-object*) ou **estego-recipiente (***stego-carrier***)**, ou seja, um arquivo com uma mensagem embutida. Uma **estego-key** (*stego-key*) ou simplesmente **chave** é utilizada para controlar o processo de esconder, assim como, para restringir detecção e/ou recuperação do dado embutido, somente para quem a conhece, ou conheça parte dela. Uma possível fórmula deste processo pode ser representada da seguinte forma:

Recipiente + mensagem embutida + estego-key = estego-objeto

O termo **recipiente** é dado a qualquer tipo de informação digital que é transmitida por um sistema digital ou analógico, assim como arquivos de texto, áudio, vídeo, figuras, por exemplo, BMP, GIF, JPEG, MP3, WAV, AVI ou outros tipos.

Visto que o objetivo da esteganografia é a ocultação, sem suspeitas, de informações dentro de outros dados, a esteganoanálise visa identificar a presença de informações ocultas.

Da mesma maneira que um criptoanalista aplica criptanálise na tentativa de decodificar ou resgatar a mensagem criptografada, o esteganoanalista aplica a esteganoanálise na tentativa de descobrir a existência de informações escondidas. Na criptografia, a comparação é realizada entre porções (possivelmente nenhuma) de *plaintexts* (texto em claro) e porções de textos cifrados. Na esteganografia, comparações são realizadas entre o estego-objeto, o recipiente e possíveis partes da mensagem. O resultado final na criptografia é o texto cifrado, enquanto que na esteganografia é o

1 First Information Hiding Workshop held in Cambridge, UK in April 1996; Anderson, R., (ed.): Information Hiding: First International Workshop, Cambridge, UK. Lecture Notes in Computer Science, Vol. 1174. Springer-Verlag, Berlin Heidelberg, New York (1996).

estego-objeto. A mensagem na esteganografia pode ou não estar criptografada, caso esteja, a mensagem é extraída e então técnicas de criptoanálise são aplicadas.

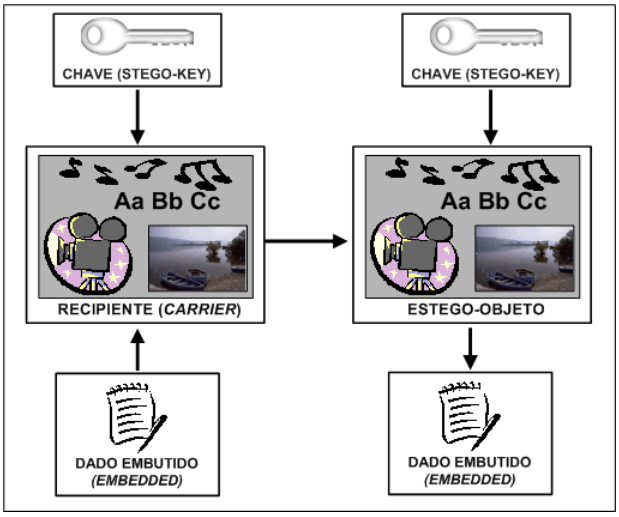


Figura 1 – Terminologia de Esteganografia

Para que o esteganoanalista possa realizar a análise, faz-se necessário o conhecimento dos seguintes componentes [23]:

- Stego-only *(apenas Esteganografia)*;
- Known cover *(recipiente conhecido)*;
- Known message *(mensagem conhecida)*;
- Chosen stego *(escolha da Esteganografia)*; *e*
- Chosen message *(mensagem escolhida)*.

O ataque *stego-only* é similar ao *ciphertext only,* onde somente o estego-objeto está disponível para análise. Se o recipiente original e o estego-objeto estão disponíveis, então um ataque *known cover* está disponível. O esteganoanalista pode utilizar um ataque *known message* quando a mensagem escondida já foi revelada anteriormente, assim um atacante pode analisar os estego-objetos para futuros ataques. Mesmo com a mensagem, este pode ser um ataque muito difícil e pode ser considerado um ataque *stego-only*. No ataque *chosen stego,* a ferramenta (algoritmo) de esteganografia e o estego-objeto são conhecidos. No ataque *chosen message,* o esteganoanalista gera o estego-objeto que aponta o uso de ferramentas ou algoritmos de esteganografia específicos.

5. HISTÓRIA

O primeiro registro conhecido sobre utilização de esteganografia está no livro "História" de Herótodo [11], por volta do ano 440 a.C., onde o tirano grego Histeu recebe do Rei Dario a cidade de Mircina como recompensa por ter protegido uma região estratégica de Trácia, uma região pertencente aos domínios de Dario. Quando Dario percebe que havia dado a Histeu uma terra rica em prata e madeira resolve retirar o Histeu do comando desta, para tanto solicita que Histeu fique ao lado do rei como seu conselheiro em Susa. Histeu, lisonjeado com o reconhecimento do rei, aceita a proposta, ficando seu enteado Aristágoras responsável pela cidade. Com o passar do tempo, Histeu descobre que se não ocorressem distúrbios naquela cidade, nunca mais voltaria a ela. Sendo assim, Histeu solicita a presença de seu escravo considerado mais fiel entre os demais. Histeu então lhe raspa a cabeça e tatua uma mensagem em seu couro cabeludo concitando Aristágoras à revolta. Quando o cabelo do escravo cresceu o suficiente ele foi enviado à cidade de Mircina, recomendando o escravo que apenas dissesse a Aristágoras que lhe raspasse a cabeça e a examinasse com atenção.

Ainda em "História" de Heródoto, consta que na Grécia antiga o meio de escrita era texto em tabletes duplos cobertos de cera. Demerato, um grego, precisava avisar Esparta que Xerxes pretendia invadir a Grécia. Como lhe faltavam meios para isso e receava ser descoberto, serviu-se do seguinte

artifício: pegou alguns tabletes duplos, raspou a cera que os cobria e neles escreveu o aviso com referências aos planos de Xerxes. Feito isso, cobriu as letras novamente com cera. Os tabletes pareciam estar em branco e sem uso, por isso passaram pela inspeção e a mensagem chegou ao seu destino da maneira que Demerato previra.

Entretanto, essa não seria a última vez que a esteganografia seria utilizada em tempos de guerras. Tintas invisíveis baseadas em substâncias como suco de frutas, urina e leite eram utilizadas para esconder informação. Até mesmo na 2ª Guerra mundial, a tecnologia mais utilizada de esteganografia eram tais tintas [16]. Também foram utilizadas cifras nulas (mensagens não criptografadas) pelos alemães para esconder mensagens secretas. As cifras nulas, que geralmente pareciam ser mensagens inocentes sobre acontecimentos ordinários, não gerariam suspeitas, não sendo então interceptadas [16]. A seguinte mensagem é um ótimo exemplo de cifras nulas (obs.: manteremos a mensagem original):

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

Decodificando essa mensagem, pegando a segunda letra em cada palavra revela a seguinte mensagem secreta:

Pershing sails from NY June 1.

A disposição do documento também costumava revelar informação. Modulando a posição de linhas e palavras, mensagens poderiam ser marcadas e identificadas [5].

Novas tecnologias que armazenavam mais informação em meios nada suspeitos foram desenvolvidas, a detecção de mensagens também foi melhorada. A invenção alemã dos micropontos foi considerada pelo Diretor do FBI, J. Edgar Hoover, como a "obra-prima da espionagem inimiga". Micropontos são fotografias do tamanho de um ponto impresso tendo a clareza de páginas datilografadas de tamanho normal, o que permitia a transmissão de grandes quantidades de dados [5].

Em termos de computação, a esteganografia evoluiu na prática de esconder uma mensagem dentro de uma maior de tal maneira que uma pessoa não pode discernir a presença ou os índices da mensagem. Em termos contemporâneos, a esteganografia evoluiu numa estratégia digital com intuito de esconder um arquivo em algum dos meios multimídia, tais como arquivos de *imagem*, de *áudio* ou de *vídeo*.

6. ESTADO DA ARTE

A prática de criptografia assume que o método utilizado para criptografar é de domínio público, e a segurança reside na escolha da chave [17]. Por analogia, é de se esperar que desenvolvedores de sistemas de esteganografia deveriam publicar os mecanismos por eles utilizados, e confiariam no segredo de suas chaves. Infelizmente não é o caso, muitos fornecedores deste tipo de sistemas armazenam o cabeçalho dos mecanismos utilizados em seus acordos de não-revelação, algumas vezes justificando a existência da patente.

6.1. Sistemas simples

Vários softwares de esteganografia estão disponíveis para embutir informações em imagens digitais. Alguns deles, simplesmente, utilizam os últimos bits significativos dos *pixels* da imagem recipiente para adicionar os bits da mensagem [21]. A informação embutida desta forma deve ser imperceptível aos sentidos humanos [19], mas é trivial para que um especialista possa detectar e destruir a mensagem.

Outros sistemas assumem que ambos, remetente e destinatário, compartilham uma chave secreta e usam um gerador convencional de chaves criptográficas [23]. A chave é então utilizada para selecionar *pixels* ou amostras de som em que os bits do texto cifrado serão embutidos [10].

No entanto, nem todo *pixel* é apropriado para codificar um texto cifrado: mudanças de *pixels* em grandes campos de cores monocromáticas, ou nos *pixels* que ficam em fronteiras definidas, podem ser visíveis ao olho humano. Alguns sistemas têm algoritmos que determinam se um *pixel* candidato pode ser utilizado, pela verificação da variação na luminosidade de *pixels* adjacentes, nem tão alta

(como numa fronteira) nem tão baixa (como em um campo monocromático). Sempre que um *pixel* passar por este teste é possível alterar seus últimos bits significativos para embutir um bit de uma mensagem.

Tais esquemas podem ser destruídos de várias maneiras por um oponente que pode modificar a estego-imagem. Por exemplo, quase todos os processos triviais de filtragem mudam o valor de muitos dos últimos bits significativos. Uma possível contramedida é utilizar redundância: alguém poderia inserir um erro corrigindo o código, ou simplesmente embutir uma marca várias vezes. Por exemplo, o algoritmo "*Patchwork*" (trabalho com retalhos) de Bender *et al.* esconde um bit em uma imagem, aumentando a variação da luminosidade de um grande número de pares de *pixels* pseudo-randomicamente escolhidos [20].

Uma forma de atacar estes sistemas é separar a sincronização necessária para localizar as amostras em que a assinatura foi escondida: figuras, por exemplo, podem ser *cropped* (corte das margens de uma foto). No caso de áudio, um simples, mas efetivo, ataque de dessincronização pode ser utilizado: randomicamente, excluí-se uma proporção pequena de amostras, e duplica-se um número similar de outras. Isto introduz um *jitter*[2] de alguns décimos de microssegundos, que é insignificante comparado à precisão com que o som original foi, na maioria dos casos, gerado, mas suficiente para confundir um típico esquema de assinatura.

Com um tom puro, é possível excluir ou duplicar, uma amostra em 8.000 *jitters*, e com uma música clássica pode-se excluir ou duplicar uma em 500, sem que o resultado seja perceptível. Utilizando os algoritmos de filtragem de reamostras, pode-se obter uma em 500 *jitters* em um tom puro, e uma em 50 no *speech*, sem transparecer a diferença. O resultado da música clássica também pode ser aumentado significativamente, mas cálculos precisos dependem da música utilizada.

6.2. Técnicas de transformação

Um problema sistemático com o tipo de esquema descrito acima é que, aqueles bits que foram embutidos com segurança em um recipiente são, pela definição, redundantes, onde um atacante desavisado sobre a alteração dos bits acredita que os mesmos podem ter sido removidos por um esquema de compressão eficiente. A interação entre compressão e esteganografia é uma linha recorrente na literatura. Quando é conhecido previamente o esquema de compressão utilizado, é possível personalizar um método de embutir para obter um resultado razoável. Por exemplo, em arquivos GIF é possível trocar cores similares (cores adjacentes na paleta atual) [13], no entanto, se quisermos embutir uma mensagem em um arquivo que pode ser sujeito à compressão JPEG e filtragem, é possível embuti-la em múltiplas localizações [25], ou melhor ainda, embuti-la no domínio de freqüência, alterando componentes da transformação do co-seno discreto da imagem.

As técnicas "*spread spectrum*" são freqüentemente combinadas às características do material recipiente. Por exemplo, um sistema de assinatura de áudio de forma que explore as propriedades de mascaramento do sistema auditivo humano [4].

Mascarar é um fenômeno em que um som interfere na percepção de outro som. O mascaramento da freqüência ocorre quando dois tons com freqüências parecidas são tocados ao mesmo tempo. O tom mais alto irá mascarar o mais baixo [12], [22]. Contudo, isto não ocorre quando tons têm freqüências distantes. Similarmente, mascaramento temporal ocorre quando um sinal de baixo nível é tocado imediatamente depois de um mais forte. Por exemplo, depois de se escutar um som muito alto, leva um tempo antes que seja possível escutar um som muito baixo.

Técnicas de compressão de áudio MPEG exploram estas características [1], além disso, é possível explorá-las inserindo assinaturas que estejam acima da truncagem do início do MPEG, e abaixo do início da percepção [4]. Geralmente, uma existência de marca d'água pode ser detectada por testes de estatística, enquanto permanecer indetectável aos humanos, a verdadeira questão é até quando pode ser danificado além da recognição, sem introduzir distorção perceptível.

[2] Fenômeno caracterizado pelo desvio no tempo ou na fase de um sinal de áudio. Pode ser responsável por erros e perda de sincronismo.

6.3. Métodos de esteganografia - Imagem

A Internet é um canal vasto para disseminação de informação. Imagens são utilizadas em toda a rede com diversos propósitos, elas provêem excelentes recipientes para esconder informações. Ferramentas de esteganografia podem ser caracterizadas em dois grupos: *Imagem de Domínio* e *Transformação de Domínio*.

Ferramentas de *Imagem de Domínio* envolvem métodos que aplicam inserção do último bit significativo e manipulação de distorção. Estes métodos são comuns na esteganografia e são caracterizados como "sistemas simples" em [2]. Ferramentas utilizadas neste grupo incluem *StegoDos, S-Tools, Mandelsteg, EzStego, Hide and Seek, Hide4PGP, Jpeg-Jsteg, White Noise Storm,* e *Steganos.* Os formatos de imagens tipicamente utilizados nestes métodos de esteganografia são de *lossless* e o dado pode diretamente ser manipulado e recuperado.

Ferramentas de *Transformação de Domínio* incluem aquelas que envolvem manipulação de algoritmos e transformação de imagens, assim como Transformação do Co-seno Discreto (TCD) [9], [18] e transformação *wavelet* [24]. Estes métodos escondem a mensagem em áreas mais significativas do recipiente e podem manipular as propriedades da imagem, por exemplo, sua luminosidade. Estas técnicas são mais robustas que as técnicas de Imagem de Domínio. Contudo, existe uma relação entre a informação adicionada à imagem e a robustez obtida [15]. Vários métodos de *Transformação de Domínio* são independentes do formato e podem suportar a conversão entre os formatos de *lossless* e *lossy*.

O método de compressão *Lossless* é utilizado quando existe uma necessidade que a informação original permaneça intacta. A mensagem original pode ser reconstruída exatamente igual. Este tipo de compressão é tipicamente utilizado em imagens GIF e BMP. Já o método *Lossy* pode não manter a integridade da imagem original, mas economiza bastante espaço em disco. Este método é tipicamente utilizado em imagens JPG e produzem ótimas compressões.

Imagens JPEG utilizam a Transformação do Co-seno Discreto (TCD) para conseguir uma compressão de imagem. O dado comprimido é armazenado como números inteiros. Contudo, o cálculo para o processo de quantização requer cálculos com ponto flutuantes que são arredondados. Os erros introduzidos pelo arredondamento definem a perda característica do método de compressão em JPEG [6].

A ferramenta de esteganografia *Jpeg-Jsteg* esconde a informação manipulando os valores de arredondamentos do coeficiente JPEG TCD. A informação é escondida em uma imagem JPEG pela modulação das escolhas de arredondamento para cima ou para baixo nos coeficientes TCD.

Uma vantagem do TCD em relação aos outros tipos de transformações é a habilidade em minimizar a aparência em forma de bloco, quando os limites de pedaços da imagem com 8x8 *pixels* se tornam visíveis.

Algumas técnicas compartilham características dos dois grupos: ferramentas de *Imagem de Domínio* e *Transformação de Domínio*. Com isso, pode-se empregar a técnica *patchwork* (trabalho com retalhos), codificação em bloco padrão [20], métodos de *spread spectrum* (espalhamento de espectro) [8] ou mascaramento [14] que adiciona redundância à informação escondida. Estas abordagens podem ajudar na proteção contra algum processamento de imagem, assim como *cropping* e rotação.

A abordagem *patchwork* utiliza uma técnica pseudo-randômica para selecionar múltiplas áreas (*patches*) de uma imagem para marcação. Cada área pode conter uma marca d'água, assim, se alguma é destruída ou recortada, as outras podem suportar.

Máscaras podem incluir imagens de domínio assim como existir um componente adicionado ou um objeto imagem. Contudo, uma máscara pode ser adicionada à imagem pelo ajuste das propriedades ou transformações da imagem, recebendo, dessa forma, características de ferramentas de Transformação de Domínio.

6.4. Um modelo geral

O modelo geral de esteganografia é: primeiro se esconde informação aplicando uma transformação ao objeto recipiente e então se altera um subconjunto de bits do objeto transformado que se torna redundante. Neste contexto, redundante significa que um subconjunto não trivial,

selecionado randomicamente, pode ser de um certo tamanho, que pode ter seus valores alterados sem ser detectado facilmente por um oponente que não sabe qual subconjunto examinar.

Mesmo realizando mais trabalho na busca pela redundância aparente, sempre existirá alguém com a habilidade criar novos modelos. Pode ser especialmente se esta pessoa estiver procurando remover uma marca d'água ou impressão digital armazenada em uma música gravada em 1997 utilizando a tecnologia disponível em 2047. Esta é a grande preocupação no caso da utilização de marca registrada, ou seja, permitir que a marca não seja retirada ou modificada, aproximadamente 70 anos depois da morte do autor, no caso de texto e 50 anos no caso de áudio [3].

7. ESTEGANOANÁLISE

A esteganoanálise visa descobrir e tornar inútil, mensagens secretas ocultas em um recipiente [14].

Ao utilizar esteganografia, a qualidade do objeto é degradada e tal degradação pode ser perceptível aos sentidos dos seres humanos [19] e demonstrar certas características semelhantes, o que torna possível padronizar uma espécie de assinatura permitindo a detecção dos métodos e dos softwares utilizados. Tais assinaturas podem acusar a existência de uma mensagem embutida, o que acaba com a finalidade da esteganografia, que é esconder a existência de uma mensagem.

Os procedimentos de ataques contra esteganografia são: detecção e destruição da mensagem embutida. Um objeto (imagem, som e vídeo) pode ser manipulado com a intenção de se destruir informações embutidas, existentes ou não. A detecção da existência de esteganografia em um objeto poupa tempo na fase da eliminação da mensagem, quando processados somente objetos que contenham dados escondidos.

A figura 7 mostra um diagrama, onde os círculos denotam onde o esteganoanalista pode obter acesso ao sistema de esteganografia. No caso de obtenção de mais de uma destas marcas, o resultado são diferentes tipos de ataques.

Uma importante distinção deve ser feita entre ataque passivo e ativo: no primeiro o esteganoanalista é capaz somente de interceptar o dado, enquanto que no segundo ele consegue interceptar e manipular o dado. No diagrama da figura 7, um círculo preenchido significa que um atacante tem acesso suficiente para realizar um ataque ativo. Se o círculo não estiver preenchido, somente é possível realizar ataques passivos.

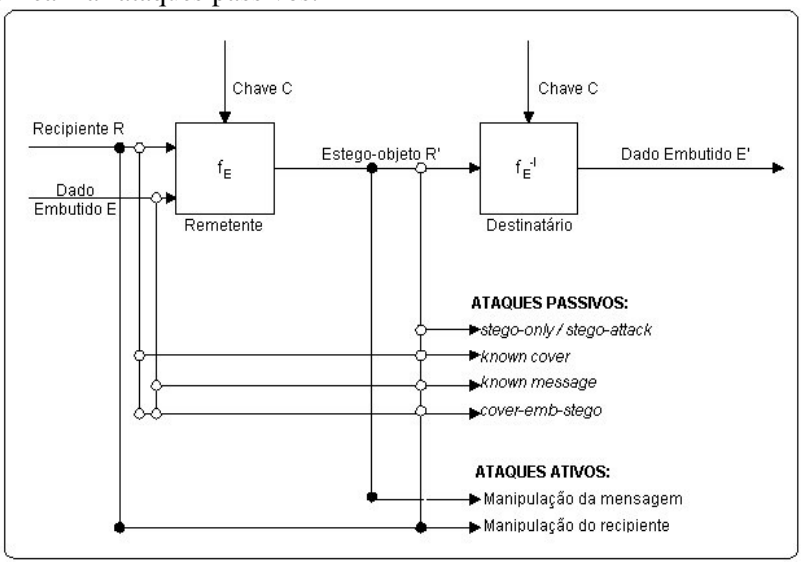


Figura 2 – Sistema de Esteganografia Ampliado

Os seguintes ataques estão disponíveis neste modelo:

- *Stego-only (apenas esteganografia):*

Somente o estego-objeto está disponível para análise. O esteganoanalista intercepta o dado e é capaz de analisá-lo.

- *Stego-attack (ataque de esteganografia):*

O remetente utiliza um mesmo recipiente repetidas vezes. O esteganoanalista possui estego-objetos diferentes que foram originados do mesmo recipiente. Em cada um destes arquivos, diferentes mensagens estão embutidas.

- *Known cover (recipiente conhecido):*

O recipiente original e o estego-objeto estão disponíveis. O esteganoanalista intercepta o estego-objeto e compara com o recipiente que foi utilizado para criar o estego-objeto.

- *Known message (mensagem conhecida):* O remetente utiliza um mesmo recipiente várias vezes. A mensagem escondida já foi revelada anteriormente, o que permite a análise de estego-objetos para futuros ataques.
- Cover-emb-stego *ou k*nown-cover-message *(mensagem e recipiente conhecidos):* O esteganoanalista intercepta o estego-objeto e conhece, não somente qual recipiente foi utilizado, mas também a mensagem que foi armazenada no estego-objeto.
- *Manipulação da mensagem:* O esteganoanalista tem habilidade para manipular a mensagem. É possível modificar ou remover a mensagem embutida.
- *Manipulação do recipiente:* O esteganoanalista pode manipular o recipiente e interceptar a mensagem. Isto é possível pela determinação dos locais do estego-objeto que contêm dados embutidos.

Os ataques *stego-attack* e *know-cover* podem ser prevenidos se o usuário do sistema de esteganografia tomar algumas precauções: não se deve utilizar o mesmo recipiente várias vezes, e também não se deve utilizar, como recipientes, arquivos que são amplamente distribuídos ou facilmente encontrados na *web*.

O ataque *stego-only* é o mais importante contra sistemas de esteganografia, pois ocorre com mais freqüência. Métodos diferentes foram desenvolvidos para determinar onde um certo estego-objeto pode conter dados escondidos. Dois diferentes métodos podem ser distinguidos: ataques visuais, que confiam nas capacidades do sistema visual do ser humano e ataques estatísticos que apresentam testes estatísticos no estego-objeto.

8. COMBINAÇÕES DE MÉTODOS PARA OCULTAR AINDA MAIS A INFORMAÇÃO

A esteganografia é simplesmente uma de muitas maneiras de proteger a confidencialidade dos dados e provavelmente a melhor usada conjuntamente com um outro método de omissão de dados. Quando usados em combinação, estes métodos podem ser parte de uma abordagem de segurança. Alguns bons métodos complementares incluem:

Criptografia – é uma ciência utilizada para codificar arquivos de maneira que somente quem possua uma chave de entrada poderá decodificar os mesmos. O objetivo básico da criptografia é tornar uma mensagem ininteligível para um adversário, que possa vir a interceptar a mensagem [7]. Ao utilizar criptografia juntamente com esteganografia é aconselhável que se realize primeiro o processo de criptografia e depois esteganografia, isto porque para um interceptador será necessário saber que dentro de algum objeto existem dados ocultos e depois de recuperá-los, será necessário quebrar o algoritmo de criptografia.

Métodos simples – alguns métodos simples também podem ser utilizados para conseguir maior confidencialidade dos dados. Renomear os nomes dos arquivos para nomes inocentes, compactá-los diversas vezes utilizando senhas e/ou disponibilizá-los em *sites* desconhecidos.

Canais secretos - algumas ferramentas podem ser usadas para transmitir dados valiosos no tráfego normal da rede. Um exemplo é a ferramenta Loki, ela esconde dados no tráfego do ICMP. É utilizada como um *backdoor* em sistemas Unix.

9. CONCLUSÃO

Diante da guerra da informação, não se sabe até que ponto é possível confiar em qualquer informação digital, até porque uma mensagem aparentemente inocente pode estar escondendo informações ou comandos de guerra/terrorismo. É preciso ponderar que armas de guerra da informação podem ser utilizadas tanto como defesa, quanto ataque.

Todas as formas de se preservar devem ser consideradas, pois sempre haverá alguém com tempo e talento suficiente para conseguir transpô-las. Contudo é necessário muita tática de defesa, obrigatoriamente contra os ataques mais conhecidos, mas também é imprescindível estudar e entender outras tecnologias, como a esteganografia, que desde antes de Cristo é utilizada, mas que quase ninguém conhece sua forma digital.

10. REFERÊNCIAS BIBLIOGRÁFICAS

[1] AMBIKAIRAJAH, Eliathamby; DAVIS A.G. WONG W.T.K. "Auditory masking and MPEG-1 audio compression" Electronics and Communication Engineering Journal (IEE). p. 165-175. August, 1997.

[2] ANDERSON, Ross J.; PETITCOLAS, Fabien A. P. "*On the Limits of Steganography"*, IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, p. 474-481. May, 1998.

[3] ANDERSON, Ross J.; PETITCOLAS, Fabien A. P.; KUHN, Markus G. "*Information Hiding - A Survey",* Proceedings of the IEEE, Volume 87, Nº. 7. July, 1999.

[4] BONEY Laurence; HAMDY Khaled N., TEWFIK Ahmed H. *"Digital Watermarks for Audio Signals"*, IEEE International Conference on Multimedia Computing and Systems. Hiroshima, Japan; pp. 473-480. June, 1996.

[5] BRASSIL, Jack; GORMAN, Lawrence O'.; LOW, S. H.; MAXEMUMCHUK N. "*Document Marking and Identification using Both Line and Word Shifting",* Proc. Infocom, IEEE CS Press, Los Alamitos, Calif., v.13. June, 1994.

[6] BROWN, W.; SHEPHERD, B.J. "*Graphics File Formats: Reference and Guide*". Manning Publications, Greenwich, CT 1995.

[7] CARVALHO, Daniel Balparda de. *Segurança de Dados com Criptografia: Métodos e Algoritmos*. Editora: book Express, 2ª ed. 2001.

[8] COX, I.; KILIAN, J.; LEIGHTON, T.; SHAMOON, T. "*Secure Spread Spectrum Watermarking for Multimedia*". Technical Report 95-10, NEC Research Institute, 1995.

[9] COX, I.; KILIAN, J.; SHAMOON, T.; LEIGHTON, T. *A Secure, Robust Watermark for Multimedia*. Lecture Notes in Computer Science 1174 p. 185-206, Springer-Verlag. June, 1996.

[10] FRANZ Elke; JERICHOW Anja; MOLLER Steffen; PFITZMANN Andreas; STIERAND Ingo. "*Computer Based Steganography: How it works and why therefore any restrictions on cryptography are nonsense, at Best"*, Information hiding: first international workshop, Cambridge, UK. Springer Lecture Notes. No. 1174. p. 7-21. 1996.

[11] HERÓDOTO. *História***.** Gráfica Editora Brasileira LTDA, São Paulo, SP, 1ª ed., 1953.

[12] HOLMES, J. N. *Speech Synthesis and Recognition-Aspects of Information Technology,* Chapman & Hall, 1993.

[13] JAGPAL G. *Steganography in Digital Images Thesis*, Cambridge University Computer Laboratory, May 1995.

[14] JOHNSON, Neil F.; JAJODIA Sushil. "*Lecture Notes*" – Lecture Notes in Computer Science, Vol. 1525, published by Springer-Verlag (1998).

[15] JOHNSON, Neil F.; JAJODIA, Sushil. *Exploring Steganography: Seeing the Unseen.* IEEE Computer. p. 26-34. February (1998).

[16] KAHN, David. *The Codebreakers,* Macmillan Publishing Co., New York State. Editora: Scribner, New York, 1996.

[17] KERCKHOFFS, Auguste. "*La Cryptographie Militaire*", Journal des Sciences Militaires, 9th series, IX , p 5-38; January 1883; p 161-191, February 1883.

[18] KOCH, E.; RINDFREY, J.; ZHAO, J. *Copyright Protection for Multimedia Data.* Proceedings of the International Conference on Digital Media and Electronic Publishing, December 1994. Leeds, UK, 1994.

[19] KURAK, Charles; MCHUGH John. "*A Cautionary Note On Image Downgrading*", IEEE Eighth Annual Computer Security Applications Conference, p. 153-159, 1992.

[20] MORIMOTO, Norishige; BENDER, Walter; GRUHL, Daniel; LU, Anthony. "*Techniques for Data Hiding*", IBM Systems Journal vol. 35 nº 3, p. 313-336, 1996.

[21] OSBORNE, C.F.; SCHYNDEL, R.G. van; TIRKEL, A.Z. "*A Digital Watermark"*, International Conference on Image Processing, (IEEE) v 2 pp 86-90, 1994.

[22] PARSON, T. *Voice and Speech Processing*, McGraw-Hill, 1986.

[23] SCHNEIER, Bruce. *Applied Cryptography-Protocols, Algorithms and Source Code in C*, 2th Edition, J. Willey, 1995.

[24] XIA, X; BONCELET, C. G.; ARCE, G. R. "*A Multiresolution Watermark for Digital Images"*. IEEE International Conference on Image Processing. October, 1997.

[25] ZHAO, Jian; KOCH, Eckhard. "*Towards Robust and Hidden Image Copyright Labeling"*, Proceedings of 1995 IEEE Workshop on Nonlinear Signal and Image Processing - Neos Marmaras, Halkidiki, Greece - June, 1995.

[26] MAGALHÃES, João; *As Epístolas de Bin Laden* – Disponível na Internet: http://www.estadao.com.br/magazine/materias/2001/out/01/314.htm

O ENFRENTAMENTO DA PORNOGRAFIA INFANTIL NA INTERNET: O PAPEL DOS CANAIS DE DENÚNCIA

Fábio André Silva Reis BSc, MA.

Assessor Técnico da Secretaria da Justiça e Direitos Humanos da Bahia
Mestre em Criminologia Internacional (Sheffield University, Inglaterra)
Bacharel em Ciência da Computação (Universidade Federal da Bahia)

Resumo

Este breve artigo versa sobre o papel dos canais de denúncia, também conhecidos como Internet hotlines, no atual contexto do enfrentamento internacional da pornografia infantil na Internet, bem como acerca da sua atuação subsidiária e complementar ao das autoridades policiais.

1. INTRODUÇÃO

A pornografia infantil na Internet é um dos crimes mais evidentes no ciberespaço. Tanto localmente quanto internacionalmente, o enfrentamento da disseminação da pornografia infantil na Internet já faz parte da agenda de diferentes governos. No Brasil, a Polícia Federal afirma que, dentre os crimes de computador, a pornografia envolvendo crianças responde pelo maior número de denúncias recebidas pela instituição[1]. Apesar da alta taxa de exclusão digital da população brasileira[2], ao menos três fatores tendem a potencializar o aumento da produção e distribuição da pornografia infantil on-line no Brasil. Primeiramente, a implementação de políticas sérias de enfrentamento à exploração sexual comercial de crianças e adolescentes na União Européia e nos Estados Unidos resulta no fortalecimento de mercados produtores em países carentes de intervenções sociais integradas e onde a exploração sexual comercial de crianças ainda é uma realidade constante, como é o caso do Brasil. Em segundo lugar, a crescente produção e barateamento de equipamentos digitais tornam cada dia mais fácil e rápido produzir grandes quantidades de áudio e vídeo digital resultantes do abuso sexual de crianças e adolescentes. Por fim, a democratização do acesso à Internet, como política de governo, representa, ao menos potencialmente, um aumento do público produtor e consumidor da pornografia infantil na Internet brasileira.

Lastreados nesse contexto de provável crescimento, desde 1998, diversos atores têm envidado esforços no sentido de desenvolver um modelo, ainda que disperso, de enfrentamento à pornografia infantil na Internet brasileira. Exemplos tais como a operação Catedral-Rio, as atividades de canais de denúncias, a aprovação de lei específica (BRASIL, 2003) e a realização de conferência internacional[3] comprovam a assertiva anterior. Entretanto, somente a partir de 2004, o Governo Federal começa a mostrar sinais de que esforços mais substanciais começam a ser empregados na construção de um plano nacional integrado de enfrentamento. Nesse caso, podemos tomar como exemplo a criação da Comissão Intersetorial, coordenada pela Secretaria Especial dos Direitos Humanos, a qual congrega diversos órgãos públicos, organismos internacionais e entidades da sociedade civil. A Comissão

[1] Conforme declaração do Representante da Polícia Federal na I Conferência Internacional sobre Pornografia Infantil na Internet, 01-04 dez. 2002, Salvador, Bahia.
[2] Aproximadamente, apenas 8,31% da população brasileira tem acesso à Internet em seus lares (FGV, 2003)
[3] I CONFERÊNCIA INTERNACIONAL SOBRE PORNOGRAFIA INFANTO-JUVENIL NA INTERNET, Salvador**. Pornografia Infanto-Juvenil na Internet, uma Violação aos Direitos Humanos.** Salvador: CEDECA-BA, 2002, 58p.

Intersetorial está dividida em cinco subcomissões; a subcomissão referente à pornografia infantil, dentre outras atividades, será responsável pela construção do Plano Nacional de Enfrentamento à Pornografia Infantil na Internet e pela articulação de atores-chave nesse enfrentamento.

Já no âmbito internacional, diversos países têm aprovado leis específicas, criminalizando a produção, a distribuição e a posse da pornografia infantil, bem como a montagem das chamadas pseudo-fotografias; autoridades policiais têm conduzido variadas operações policiais internacionais de forma conjunta; e canais de denúncia têm se agrupado em associações internacionais de forma a favorecer a troca de informações. Por exemplo, o INHOPE Forum[4], apesar de congregar atualmente membros de dezoito países, pretende ampliar o número de nações associadas, demonstrando a preocupação internacional com o tratamento do problema (INHOPE, 2004).

Conforme observado, a proliferação da pornografia infantil na Internet têm recebido atenção por parte dos governos nacionais; tal fato se deve, em grande parte, ao papel da mídia na construção do tema. Ela tem representado a Internet, com certa freqüência, como um grande mercado da pornografia infantil (MACHIL e REWER, 2001: 49), colocando o assunto na agenda social, construindo consensos e fornecendo suporte para a regulação do ciberespaço e criminalização da produção, distribuição e consumo da pornografia infantil (OSWELL, 1998: 274). Contudo, as representações da mídia usualmente exageram a ameaça do crime promovendo a punição e policiamento como antídotos naturais (REINER, 2002: 407).

Ademais, as pessoas estão atualmente tão imersas em uma cultura de riscos e medos (DOUGLAS, 1992: 29) que a identificação e o gerenciamento de riscos tornam-se princípios basilares da vida social (LOADER e SPARKS, 2002: 94). E onde há riscos e medos, é necessário construir confiança, bem como uma cultura de responsabilidades (MACHILL e REWER, 2001: 49). Conseqüentemente, promove-se o compartilhamento de responsabilidades na gerência desses riscos, mediante a criação de um modelo co-regulatório. Em outras palavras, o Estado sozinho não possui condições materiais e humanas para regular um ambiente complexo como a Internet e, portanto, compartilha a gerência dos variados riscos pertinentes com diversos atores sociais. Assim, polícia, provedores de acesso e conteúdo, canais de denúncia, mídia, usuários de Internet, legisladores, poder judiciário e organizações de proteção aos direitos das crianças e dos adolescentes; todos eles desempenham papéis complementares no enfrentamento à pornografia infantil na Internet (OSWELL, 1999: 44; OSWELL, 1998: 275; EDWARDS, 2000: 290; WALL, 2001: 167).

Vale salientar que iniciativas de co-regulação envolvem o comprometimento mútuo dos parceiros, os quais compõem uma rede de responsabilidades compartilhadas onde os governos dos países e os (as) usuários (as) de Internet possuem funções essenciais. Como resultado, iniciativa privada, sociedade civil, pais, mídia, autoridades policiais, usuários de Internet e governo são definidos como agentes responsáveis em uma nova cultura de responsabilidades (MACHILL e REWER, 2001: 48; MACHILL e WALTERMANN, 2000: 11; PRICE e VERHULST, 2000: 134). Não causa surpresa, portanto, que diversas nações do mundo tenham desenvolvido modelos reguladores do conteúdo on-line, os quais envolvem o monitoramento pró-ativo e reativo por parte da polícia e dos provedores de acesso à Internet, o desenvolvimento de filtros eletrônicos, a criação de códigos de conduta para provedores de acesso e conteúdo, a efetiva produção legislativa, o monitoramento parental, a maior visibilidade dada pela mídia e a criação de canais de denúncia, também chamados de Internet hotlines (MACHILL e WALTERMANN, 2000: 16).

2. CANAIS DE DENÚNCIA OU INTERNET HOTLINES

Um canal de denúncia ou Internet hotline (IH) representa um serviço de recebimento e processamento de denúncias referente a conteúdo ilegal disponível na Internet. Eles recebem

[4] INHOPE Association of Internet Hotlines Providers. Homepage Institucional. Disponível em: <http://www.inhope.org>. Acesso em: 21 mai. 2004.

denúncias relativas à existência, v.g., de pornografia infantil na Internet e, após avaliação prévia acerca da possível ilegalidade e provável origem do material denunciado, enviam a denúncia recebida para a polícia competente e requerem a retirada do material aos provedores de acesso ou conteúdo pertinentes (WILLIAMS, 1999: 8). Vale citar que os canais de denúncia possuem características diferenciadas no tocante à sua estrutura, objetivos institucionais e nível de articulação a depender do país onde estejam operando (INHOPE, 1999).

O hotline é um canal de comunicação que conecta diferente atores dentro de um modelo co-regulatório (BURKERT, 2000: 265) composto por provedores de acesso e conteúdo, canais de denúncia internacionais, associação de canais de denúncia, autoridades policiais, mídia, organizações de proteção aos direitos das crianças e dos adolescentes, bem como usuários de Internet e legisladores. De acordo com Machill e Rewer (2001: 59), IHs também evitam uma reação governamental exagerada a outros tipos de material que são meramente ofensivos, mas legais. Burkert ainda afirma que os canais de denúncia contribuem para o processo de aprendizado social de uma nova mídia, sobre a qual temos ainda de aprender quando e em quem confiar (2000: 269).

De uma forma crescente, canais de denúncia têm exercido um papel crucial no monitoramento da pornografia infantil disponibilizada on-line (MACHILL e REWER, 2001: 47. De fato, diferentes hotlines europeus recebem atualmente um suporte financeiro substancial proveniente da União Européia (2001); vale citar que a referida entidade patrocina um estudo comparativo, via Universidade de Trento na Itália, com vistas a aperfeiçoar o trabalho dos IHs europeus (DAPHNE, 2001). Ademais, os governos canadense e estadunidense investem consideráveis quantias financeiras nos seus respectivos hotlines como forma de enfrentar a pornografia infantil de crianças e adolescentes na Internet (CANADA, 1999). Entretanto, essa grande aceitabilidade das atividades dos IHs não está imune a algumas críticas dirigidas à sua natureza quase judiciária e sua auto-legitimação, além da falta de mecanismos de responsabilização e dos prováveis planos de regulação no tocante a outras formas menos contenciosas de conteúdo, como por exemplo, material ofensivo legal que não constitui ilícito penal (AKDENIZ, 2001: 124; WALL, 2001: 178).

Vale ainda lembrar que as atividades de um canal de denúncias podem não se resumir ao recebimento e processamento de denúncias, mas prolongam-se nas áreas de mobilização e desenvolvimento de políticas públicas. Tomando o exemplo do canal de denúncia desenvolvido pelo CEDECA-BA, a instituição realizou em dezembro de 2000, mediante parceria com a Polícia Federal, Interpol e UNICEF, uma mesa-redonda com especialistas da Interpol-França e Polícia Federal brasileira. O Hotline CEDECA-BA também participou do II Congresso Mundial contra a Exploração Sexual Comercial de Crianças e Adolescentes em Yokohama, Japão; da Conferência Internacional sobre a Pornografia Infantil na Internet em Balsthal, Suíça; bem como do Encontro Anual do INHOPE em Roma, Itália. Em dezembro de 2002, realizou a I Conferência Internacional sobre a Pornografia Infantil na Internet em Salvador-BA, convidando especialistas de diversos países. Durante 2002, realizou cursos de informativos sobre o problema para professores da rede pública de ensino da cidade do Salvador-BA e desenvolveu um sítio na Internet sobre o tema[5]. Atualmente, a instituição participa da coordenação, juntamente com outras entidades, da implementação do plano de ação nacional de enfrentamento à pornografia infantil na Internet.

3. CANAIS DE DENÚNCIA E AUTORIDADES POLICIAIS

Os canais de denúncia, apesar da forte ligação com autoridades policiais, não são polícia, nem possuem poder de polícia. Eles realizam uma atividade subsidiária ao das autoridades policiais; devem, portanto, possuir vigorosos vínculos com essa instituição. Dentre algumas vantagens oriundas da parceria entre autoridades policias e canal de denúncia, podemos listar: a filtragem prévia de denúncias, a aceleração do contato internacional, a participação da sociedade civil e a construção de uma importante base de dados quantitativos e qualitativos.

[5] Diga Não à Pornografia Infantil na Internet. Homepage. Disponível em: <http://www.violenciasexual.org.br/porninf/>. Acesso em: 21 mai. 2004.

Grande parte das denúncias recebidas por IHs espalhados pelo mundo não diz respeito ao conteúdo ilegal, mas sim a conteúdo ofensivo. No momento em que os canais de denúncia realizam essa filtragem e processamento[6] prévios e encaminham para a polícia somente as denúncias potencialmente ilegais, em consonância com o ordenamento jurídico do país, as autoridades policiais possuirão maior tempo para se concentrar na investigação de denúncias realmente procedentes. Ademais, o trabalho dos canais de denúncia acelera o processamento de denúncias de âmbito internacional. Se por exemplo, um IH brasileiro recebe denúncia de material hospedado na Inglaterra e a encaminha diretamente ao hotline inglês, em lugar de encaminhá-la para a autoridade policial brasileira, que por sua vez encaminhará para a Interpol-Brasil, que encaminhará para a Interpol-Inglaterra, que dará prosseguimento mediante as vias policiais locais inglesas, teríamos uma via menos burocrática a percorrer. É bem mais rápido enviar as denúncias para IHs parceiros no país onde o material ilícito está hospedado, os quais já conhecem as vias idôneas de encaminhamento, do que escolher a via burocrática da comunicação policial entre os países.

Já foi evidenciado que as atividades do hotline podem não se limitar ao processamento e encaminhamento de denúncias, mas poderão também englobar atividades de conscientização, produção científica e fomento do debate em torno das possíveis políticas de enfrentamento. Os canais de denúncias são, portanto, uma fonte de participação da sociedade civil, no momento em que são estruturados de forma a se tornarem sensíveis aos mais diversos setores da sociedade. O hotline inglês Internet Watch Foundation (IWF)[7] apesar de ter sido fundado pela indústria da Internet, possui atualmente uma estrutura que contempla representantes de entidades de proteção à infância e juventude, usuários de Internet, academia, bem como um conselho de agentes financiadores.

Os dados quantitativos e qualitativos coletados no decorrer da operação dos canais de denúncia, tratados de forma comparativa e internacional através associações de IHs são repositórios importantes que poderão auxiliar futuras intervenções na área do enfrentamento da pornografia infantil na Internet. Ademais, poderão contribuir para o aprimoramento das técnicas comparativas internacionais de dados estatísticos criminais gerados em diferentes nações a partir de diferentes contextos sociais e culturais. Vale salientar que a comparação internacional dos dados estatísticos oriundos do sistema criminal é atualmente um componente de substancial importância na pesquisa criminológica internacional (BARCLAY e TAVARES, 2002). Vale ainda citar exemplos de sucesso advindos da cooperação entre autoridades policiais e canais de denúncias, tais como, a Operação Hamlet na Suécia, o trabalho do hotline Protegeles na Espanha, o desencadeamento de operações policias na Holanda a partir do trabalho do canal de denúncia Meldpunt, além da constante troca de informações e expertise entre o hotline IWF e a polícia inglesa (INHOPE, 2004: 10).

4. CONCLUSÃO

A evidência que a disseminação da pornografia infantil na Internet tem recebido ao redor do mundo, a coloca como um dos crimes mais proeminentes do ciberespaço. Como resultado, diferentes nações têm construído modelos co-regulatórios, compartilhando responsabilidades, de forma a efetivar o devido enfrentamento do problema. À luz dessa política internacional de controle do conteúdo ilegal disponibilizado on-line, as autoridades policiais encontram nos canais de denúncia, parceiros importantes para responder à proliferação da pornografia infantil na Internet de forma eficiente.

Por fim, cabe tecer uma breve comparação entre as políticas de enfrentamento desenvolvidas no Inglaterra e no Brasil no intuito de salientar que muito ainda haverá de ser realizado no nosso país, no tocante ao tratamento do problema. A Inglaterra tem sido um país precursor na construção de iniciativas de enfrentamento à pornografia infantil, congregando esforços de importantes atores sociais desde 1996. O país possui atualmente um dos canais de denúncia mais eficientes do mundo (IWF), a

[6] O processamento envolve também a identificação da provável origem do conteúdo denunciado
[7] IWF. Homepage Institucional. Disponível em: <http://www.iwf.org.uk>. Acesso em: 21 mai. 2004.

polícia inglesa coordenou uma das maiores operações policiais internacionais de enfrentamento à pornografia infantil na Internet (Operation Cathedral), o poder legislativo já produziu uma série de dispositivos legais avançados para punir esse crime, sendo ainda importante citar a extensa produção científica sobre tema[8].

Em contraponto a esse modelo relativamente avançado, o mapa do enfrentamento da pornografia infantil na Internet brasileira é ainda uma grande incógnita; apesar dos esforços, sobretudo da sociedade civil, em trazer o tema para a agenda pública desde 1999, não há ainda no país uma política integrada e articulada entre o poder público e sociedade para afrontar o problema. Ademais, o Brasil carece de estudos sobre como as atividades têm sido desenvolvidas por instituições-chave de enfrentamento, v.g., canais de denúncias, poder legislativo, polícia e provedores de acesso e conteúdo, mídia e poder judiciário, seja isoladamente ou em conjunto. Não há estudos sobre: como os canais de denúncia têm operado; como o poder legislativo tem reagido ao problema; como a polícia tem investigado as denúncias que lhes são encaminhadas; como os provedores de acesso e conteúdo têm aplicado seus códigos de conduta; como a mídia tem representado o problema; ou como o poder judiciário tem julgado os casos investigados.

5. REFERÊNCIAS BIBLIOGRÁFICAS

AKDENIZ, Yaman. Controlling Illegal and Harmful Content on the Internet. In: Wall, David (ed) **Crime and the Internet**. p.113-39. London: Routledge. ISBN: 0-415-24428-5. 2001.

BARCLAY, G. e TAVARES, C. International **Comparisons of Criminal Justice Statistics 2000**. Home Office Statistical Bulletin Issue 05/02. London: Home Office. 12 jul. 2002.

BRASIL. **Lei nº 10.764 de 12 de novembro de 2003**. Altera a Lei nº 8.069, de 13 de julho de 1990, que dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências.

BURKERT, Herbert. The Issue of Hotlines. In: Machill, Marcel and Waltermann, Jens (eds) **Protecting Our Children on the Internet: towards a new culture of responsibility**. Gütersloh: Bertelsmann Foundation Publishers. p. 263-318. ISBN: 3-89204-474-0. 2000.

CANADÁ. **Illegal and Offensive Content on the Internet: the Canadian strategy to promote safe, wise and responsible Internet use**. Ottawa : Information Distribution Centre. 1999. ISBN: 0-662-65320-3. Disponível em: <http://www.connect.gc.ca/cyberwise/>. Acesso em: 06 abr. 2003

DAPHNE. **Daphne Programme**. Disponível em: <http://europa.eu.int/comm/justice_home/project/daphne/>. Acesso em: 06 abr. 2003.

DOUGLAS, Mary. **Risk and Blame: essays in cultural theory**. London: Routledge. ISBN: 0-415-06280-2. 1992.

EDWARDS, Lilian. Pornography and the Internet. In: Edwards, Lilian and Waelde, Charlotte (eds) **Law and the Internet: regulating cyberspace**. 2nd edition. Oxford: Hart Publications. p. 275-308. ISBN: 1-84113-141-5. 2000.

FGV. **Mapa da Exclusão Digital**. São Paulo: Centro de Políticas Sociais da Fundação Getúlio Vargas. Abril de 2003.

INHOPE. **Inhope Internet Hotline Providers: Second Report**. Disponível em: <http://www.inhope.org/doc/inhope_report_2004.pdf>. Acesso em: 21 mai. 2004.

_____ **Association of Internet Hotline Providers in Europe.** Disponível em: <http://inhope.org/english/about/members.htm>. Acesso em: 07 abr. 2003.

LOADER, Ian e SPARKS, Richard. Contemporary Landscapes of Crime, Order, and Control: governance, risk, and globalization. In: Maguire, Mike; Morgan, Rod and Reiner Robert (eds) **The Oxford Handbook of Criminology**. 3rd ed. Oxford: Oxford University Press. pp.83-111. ISBN: 0-19925609-8. 2002.

[8] Vide Cyberlaw Research Unit localizada na Universidade de Leeds. Disponível em: <http://www.leeds.ac.uk/law/cyberlaw/cyb-indx.htm>. Acesso em: 21 mai. 2004.

MACHILL, Marcel e WALTERMANN, Jens. Introduction. In: Machill, Marcel and Waltermann, Jens (eds) **Protecting Our Children on the Internet: towards a new culture of responsibility.** Gütersloh: Bertelsmann Foundation Publishers. p. 9-21. ISBN: 3-89204-474-0. 2000.

MACHILL, Marcel e REWER, Alexa. **Internet-Hotlines: evaluation and self-regulation of Internet content.** Gütersloh: Verlag Bertelsmann Stiftung. ISBN: 3-89204-555-0. 2001

OSWELL, David. The Dark Side of Cyberspace: Internet content regulation and child protection. **Convergence**, 5(4), p.42-62. 1999.

_____ The Place of Childhood in Internet Content Regulation: A Case Study of Policy in the UK. **International Journal of Cultural Studies**,1(2), p.271-91. 1998.

PRICE, Monroe e VERHULST, Stefaan. The Concept of Self-Regulation and the Internet. In: Machill, Marcel and Waltermann, Jens (eds) **Protecting Our Children on the Internet: Towards a New Culture of Responsibility.** p.133-98.ISBN 3-89204-474-0. 2000.

REINER, Robert. Media Made Criminality. In: Maguire, Mike; Morgan, Rod and Reiner Robert (eds) **The Oxford Handbook of Criminology**. 3rd ed. Oxford: Oxford University Press. pp.376-416. ISBN: 0-19925609-8. 2002.

UNIÃO EUROPÉIA. **Internet Action Plan**. 2001. Disponível em: <http://www.europa.eu.int/information_society/programmes/iap/projects/hotlines/index_en.htm>. Acesso em: 06 abr. 2003.

WALL, David. Cybercrimes and the Internet. In: Wall, David (ed) **Crime and the Internet**. London: Routledge. p.1-17. ISBN: 0-415-24428-5. 2001.

WILLIAMS, Nigel (1999) **The Contribution of Hotlines to Combating Child Pornography on the Internet.** 1999. Disponível em: <http://www.childnet-int.org/downloads/combating child pornography.pdf>. Acesso em 24 jul. 2003.

UMA SOCIOLOGIA DOS HACKERS: ASPECTOS RELEVANTES PARA O COMBATE AOS DELITOS INFORMÁTICOS NO CONTEXTO BRASILEIRO

Ariel Gomide Foina, Doutorando em Sociologia pela Universidad de Salamanca

A proposta deste ensaio é apresentar as constatações feitas por Jordan e Taylor (1998) que se considera relevante para os agentes públicos que lidam com os delitos de informática, adequando-as aos dados empíricos relativos aos membros do submundo computacional brasileiro, em especial, os membros cujas condutas se converterão em crimes com a aprovação do Projeto de Lei 84/99 (PL 84/99). Para tal segue-se uma breve análise do atual texto do referido PL e do cruzamento destas constatações supracitadas com o que se apresenta de dados teóricos e empíricos sobre o submundo computacional brasileiro, se elaborando, ao final, uma proposta de intervenção social, apresentada aqui em linhas gerais.

1. TERMOS E DEFINIÇÕES

Definir o que designa o termo "hacker" é algo que deve ser feito com cuidado. O "Jargon File" (RAYMOND, 1996) vem defini-lo num sentido de ser este alguém, geralmente num contexto de programação e desenvolvimento de software, que pratica algo pelo simples prazer de praticar. Jordan e Taylor (1998) definem a "comunidade hacker"[1] como a comunidade da qual resultam as invasões de sistema. Dentre os entes governamentais, alguns, como o *National Infrastructure Protection Center* (VATIS, 1999) nos Estados Unidos ou o *National Infrastructure Security Coordination Centre* (NISCC, 2002) no Reino Unido, referem-se, com o termo Hacker, a um indivíduo criminoso que pratique delitos de informática.

Outros como o *Interpol European Working Group on Information Technology Crime* (IEWGITC, 2002), na tentativa de resolver a questão, apresentam uma distinção entre o que seria o "Hacker White Hat", uma espécie de hacker que atua em prol da sociedade, e o "Hacker Black Hat", que seriam, estes últimos, os praticantes de crimes de informática.

Levy (2001) apresenta o termo como oriundo de um contexto histórico, referindo-se a uma filosofia de trabalho. É neste mesmo contexto que ele é empregado pelos membros da comunidade de software livre (e mais recentemente também pelo Ministério da Cultura (GIL, 2003)), em sua maioria programadores, que se auto-intitulam hackers (STALLMAN, 2002), e denominam os praticantes de invasão de sistemas pelo termo "cracker"[2].

Para evitar a polêmica em torno do termo, tomar-se-á aqui, como ponto de partida, o conceito de Jordan e Taylor (1998), uma vez que esse denomina os hackers por ações relevantes para os leitores deste artigo e principalmente quanto à constatação dos autores de que as invasões são produto não de indivíduos isolados mas sim de uma comunidade (idem). Porém, para facilitar o entendimento do texto, no decorrer deste artigo se evitará a palavra "hacker" empregada de maneira isolada, dando lugar, a expressão "Hackers Invasores".

No entanto, não se pode ignorar um elemento importante, manifesto no sentido em que o termo hacker fora empregado pelo Mistério da Cultura, e por Levy, de modo que, se fará referencia à "Sub-Cultura Hacker" sempre que o texto tratar da cultura e da ética do trabalho (HIMEMAN, 2001) compartilhada por diversas outras comunidades que atuam dentro da Internet e que em alguns casos se

1 "Hacking Community" no original.

2 Nota-se que o uso deste termo é arbitrário e se define por diferenciação e não corresponde ao uso do termo pelos membros da comunidade de crackers (um sub-grupo do submundo computacional) cuja auto-definição em nada tem a ver com qualquer tipo de atividade de invasão de sistemas mas sim com desenvolvimento de determinado tipo de software (OxEn TRSh, 2002), cujas habilidades incluem conhecimentos de programação, interpretação de linguagem de programação de baixo nível e, em alguns casos, com a prática de técnicas de engenharia reversa, mas que compartilham da sub-cultura hacker.

auto-denominam hackers (STALLMAN, 2002), mas cuja atividade central não tenha relação com invasão de sistemas ou outros delitos informáticos, como é o caso da comunidade de desenvolvedores de software livre e de alguns profissionais da indústria de segurança de informação.

Este ensaio, também não se limita a termo hacker, e opta por utilizar o termo "submundo computacional"[3] (MEYER, 1986; JORDAN e TAYLOR, 1998), o qual se refere a uma comunidade mais amorfa, que tem no uso de computadores e na conduta desviante os aspectos centrais de suas atividades. Tal termo, portanto, é mais amplo que os anteriores e se refere a diversas comunidades que coexistem, que se relacionam com certa intensidade e que, na ocasião de sua definição, incluiria não só os hackers, mas também os "Software Pirates" e os "Phone Phreackers" (universo esse que hoje certamente é mais amplo e diversificado) de modo a determinar as fronteiras, se existirem e se forem sociologicamente relevantes, entre as comunidades de hackers invasores (conforme entende Jordan e Taylor) e outros grupos, sejam os dos hackers segundo Levy, sejam os dos "Hackers White Hat", dos "Hackers Black Hat" ou dos "Crackers".

2. A SOCIOLOGIA DOS HACKERS DE JORDAN E TAYLOR E O CONTEXTO BRASILEIRO

Em estudo anterior, feito sobre a comunidade de hackers invasores, foi possível identificar várias características deste objeto de estudos. Este artigo, porém, se limitará a abordar as que se considera de maior relevância para os propósitos do mesmo, a citar: Sigilo, Anonimato, Fluidez de Fronteiras, Motivação e a relação com a indústria de segurança de informação[4].

A relação da comunidade de hackers invasores com o sigilo e o anonimato é ambivalente (Jordan e Taylor, idem). Por um lado, pode-se dizer que é natural de seu comportamento dissociar a identidade que tem fora do ciberespaço, da que tem dentro, de modo a manter a sua identidade externa oculta. Por outro lado, a identidade interna, o seu nome enquanto hacker, necessita de encontrar formas de obter reconhecimento social de seus atos enquanto os mantém encobertos de modo a não atrair, nem para si nem para seus atos, a atenção de instituições e agentes de aplicação da lei. Esse reconhecimento social, por sua vez, pode vir tanto por uma certa publicidade dada ao ato quanto pela troca de experiências com outros membros de sua comunidade.

Especificamente no Brasil, o que ocorre é que, ao que parece, por motivos mais culturais que legais, surge uma ampla comunidade hacker que não se preocupa em manter os resultados de seus atos encobertos, diferente do que aponta os autores aqui em analise, fazendo com que nosso país tome destaque internacional nos debates sobre cibercrimes. É o caso especifico da comunidade de "defacers"[5] brasileiros, grupo sobre o qual voltaremos a falar mais adiante.

A Fluides Social é outra característica que se considera relevante ao contexto Brasileiro. Os autores apontam que existe um fluxo de indivíduos e uma mudança de membros constantes. Apontam como possível razão para tal, dentre outras, o fato de ser a comunidade hacker uma rede social informal.

No contexto Brasileiro, não se identifica diferença significativa de tal modo que a informalidade e a estrutura social em rede se repetem. Nos deteremos um pouco na questão da estrutura social de rede por julgar-se este tema de especial relevância para os leitores deste artigo.

Para Castells (2003), um dos sociólogos mais importantes no que se refere ao tema das redes sociais, este tipo de estrutura tem por característica um alto grau de flexibilidade e escalabilidade e um baixo nível de hierarquização. Por flexibilidade se entende a capacidade da rede de redefinir seus objetivos ou seu modo de funcionamento em função de mudanças ambientais, um exemplo de mudanças ambientais poderia ser a provação do PL 84/99. Por escalabilidade e baixo grau de hierarquização se quer dizer que uma rede pode alterar drasticamente seu tamanho sem que isso seja prejudicial à mesma, uma vez que esta não tem uma estrutura hierarquizada, ou seja, não há um

3 "Computer Underground" no original.

4 "Secrecy", "Anonimity", "Bondary Fluidity", "Motivation" e "bond to the computer security industry ", no original.

5 "defacer", do inglês, se refere ao indivíduo que pratica o "deface", que pode ser traduzido por "desfiguração" e se refere a um tipo de ataque especifico.

controle central, uma cabeça, que coordene as ações da rede desde um centro, porque em uma rede não há centro.

Ainda segundo esse autor, uma rede é mais importante que os nós que a compõe porque um nó da rede é sempre substituível uma vez que a rede pode se reproduzir a partir de um único nó, já que cada nó da rede tem em si os elementos necessários para iniciar novas conexões que visem restabelecer-la enquanto rede.

Se estamos tratando de um objeto concreto, a comunidade de hackers invasores, e se este grupo social esta estruturado em rede, se, com o advento de uma lei de crimes informáticos, quisermos destruir essa rede, devemos levar em conta que uma rede social, do ponto de vista teórico, pode ser eliminada por dois meios. O primeiro é eliminando todos os nós da rede, o que tem como conseqüência a perda patrimonial, o que, em termos práticos, corresponderia a prender instantaneamente todos os indivíduos que a compõe perdendo-se assim o capital cultural e humano correspondente a esses nós. O segundo meio é atacando a infraestrutura de conexões, eliminando assim a rede, o que seria praticamente inviável se levarmos em conta as garantias constitucionais dos indivíduos, que são os nós desta rede, quanto a sua liberdade de expressão e comunicação e a natureza do próprio meio onde esta rede esta inserida, o ciberespaço.

Interrompendo a questão das redes e voltando a Jordan e Taylor, o aspecto motivacional não se constitui como algo absolutamente claro. Destaca-se portanto alguns dos elementos que os autores identificaram em seu trabalho de campo, a citar: curiosidade de saber o que se pode encontrar na rede; a possibilidade de se sentir detentor de poder mediante invasão de sistemas de segurança supostamente impenetráveis; reconhecimento social entre seus pares e; a crença de estarem prestando um serviço útil a sociedade e aos futuros usuários de software.

Desses elementos, se pode derivar o último aspecto daqueles autores que se pretende abordar neste artigo, a relação entre a comunidade de hackers invasores e a indústria de segurança de informação.

Jordan e Taylor apontam a existência de uma linha muito tênue separando ambas comunidades. De certo modo, a existência de uma ao mesmo tempo justifica e ameaça a existência da outra. Justifica por que uma existe para produzir os efeitos sobre os quais a outra atua ou fica impedida de atuar, e ameaça porque de um lado a comunidade de segurança da informação postula que os hackers são um mal que deve ser combatido e por outro, os hackers invasores defendem que a comunidade de segurança da informação não oferece segurança e que eles portanto prestariam um importante serviço a sociedade.

De fato, existe um fluxo de membros de um grupo ao outro. Dentre outros motivos apontados por outros autores se pode destacar a substituição de elementos motivacionais como reconhecimento social e sentimento de detenção de poder, que, no caso dos profissionais de segurança de informação, pode se dar pelo pagamento de um salário o qual, ao mesmo tempo, cumpre função de manifestar reconhecimento e de ser meio de obtenção de símbolos de poder.

Uma vez situado o leitor em parte da discussão teórica sobre o tema, passar-se-á a abordar pontos mais empíricos e específicos do contexto brasileiro.

3. CONDUTAS CRIMINALIZÁVEIS PELO PL 84/99

Várias são as leis penais aplicáveis ao ciberespaço. Em verdade, praticamente todos os tipos penais são passíveis de serem aplicados a determinadas condutas típicas realizadas dentro ou por meio da Internet. Em alguns casos os novos projetos de lei apenas vem para legislar sobre o já legislado (SILVA NETO, 2002). Em especial, crimes de ameaça, crimes contra a honra e crimes como extorsão e estelionato já vêm sendo combatidos independente da existência de legislação especial que tratasse dos cibercrimes.

Alguns tipos penais porém, como o delito de furto, devido a toda uma principiologia da aplicação da lei penal no ordenamento jurídico pátrio, não alcançavam os bens acessíveis pelo ciberespaço.

O PL 84/99[6], recentemente encaminhado para o Senado Federal sob a nova numeração de PLC 89/03 surge para corrigir esses problemas, bem como para criminalizar condutas especificas do ciberespaço que atentem contra o interesse da sociedade.

Das alterações propostas pelo projeto de lei, se tratará aqui especificamente das redações dos artigos 154-A e 266. Não se tratará aqui das demais redações propostas, dentre outros motivos, pois: para o caso do § 2º do artigo 163 e do parágrafo único do 298, entende-se que se trata de uma mera atualização da lei; no caso do 163 § 3º o texto ainda se mostra internamente contraditório, impedindo que se identifique claramente até que ponto e exatamente quais condutas serão criminalizadas de modo que se esperará as possíveis alterações que o mesmo possa sofrer no Senado antes de sua aprovação; e, para o caso do 265, se observarmos empiricamente como se dão as ações dos hackers invasores, a conduta descrita neste artigo, nestes caasos, sempre será crime meio para o 266 ou se torna algo cuja ocorrência de fato não é quantitativamente significativa.

O artigo 154-A, como proposto no projeto de lei, deixa boa margem a interpretação. Introduz no sistema penal a conduta de acessar sem defini-la. Certamente a jurisprudência tratará de aplicar a lei ao que seja razoável uma vez que todos os computadores que fazem parte da Internet, de certo modo, acessam outros computadores sem autorização.

O que interessa a este artigo é que a conduta de se ter disponível para si o conteúdo de um endereço web de modo que se possa altera-lo sem autorização ou até mesmo ciência dos responsáveis ou proprietários do mesmo, alteração essa que quando ocorre é conhecida como desfiguração[7], será uma conduta que passará a ser crime. Será crime de uma forma ou de outra, quer queira pelo próprio artigo 154-A ou pela possibilidade de se enquadrar a conduta como dano a coisa eletrônica, seja como for, criminaliza a conduta da comunidade de "defacers", um sub-grupo do submundo computacional.

O artigo 154-B, por sua vez criminaliza o porte e a negociação de endereços eletrônicos obtidos sem a autorização de seus proprietários, de modo que permite atuar contra os "spammers"[8] indivíduos que praticam "SPAM". Tal criminalização, mesmo sendo interessante pela sua originalidade até mesmo em termos de direito comparado, não interessa muito à sociologia uma vez que não há indícios de que os spammers atuem em grupos uma vez que este tema ainda carece de investigação científica.

4. ESBOÇOS CRIMINOLÓGICOS DA INVASÃO DE SISTEMAS: DEFACERS E CHAPÉUS COLORIDOS

A comunidade de "defacers" brasileiros, um sub-grupo da comunidade de hackers invasores que compartilha a sub-cultura hacker, é o grande motivo pelo qual hoje, há uma pressão mundial sobre o Brasil no sentido de controlar o cibercrime. Nossa comunidade de "defacers" é a mais ativa do mundo (MI2G, 2002) o que faz com que o Brasil receba a fama de ser um pais sem controle sobre o cibercrime (SMITH, 2003). De fato, temos sim o maior volume de invasões do tipo desfiguração originárias de grupos brasileiros, mas, se formos levar em conta o potencial ofensivo, tanto em termos de bens jurídicos quanto em termos de valores patrimoniais, o Brasil é superado por países como Rússia e Ucrânia, onde a associação entre hackers e o crime organizado parece ter resultado em uma produção em série de crimes com alta capacidade de lesão a bens juridicamente tutelados.

O ataque do tipo desfiguração tem determinadas características as quais tornam-los ponto de referência especialmente interessante para estudos de sociologia do desvio e de criminologia sobre a comunidade de hackes invasores brasileira. A desfiguração é, no ciberespaço, uma conduta muito análoga a pichação de paredes, comum em ambientes urbanos, e se define pelo ato de um hacker entrar em uma página web e trocar sua apresentaçao, sua "cara", por outra qualquer. Tal tipo de ataque, nos é de interesse por que dificilmente um proprietário ou um administrador de uma página web consegue ocultar o fato de se ter sido vítima deste tipo de ataque, o que reduz sensivelmente a

6 Quando se faz referencia ao projeto de lei, se trata do ultimo texto que se teve acesso e corresponde ao substitutivo ao projeto de lei nº 84-B, de 1999, apensos os PLs nº 2.557/00, 2.558/00 e 3.796/00, adotado em novembro de 2003.

7 "deface" do inglês.

8 "spammers" do inglês, se refere àquele que pratica o SPAM, que por sua vez, corresponde ao envio não solicitado, geralmente em massa, de correspondência eletrônica.

possibilidade de, na captação dos dados de pesquisa, nos encontrarmos presos ao debate das cifras negras, tão apontado por criminologos em outros tipos de estudos desta seara acadêmica, uma vez que com relação a outros tipos de ataque a taxa de ocultação pode chegar a 80% (KELLERMANN, 2002).

Uma vez que não se consegue ocultar tal tipo de ataque, se podem levantar diversas analises tanto de motivação, uma vez que o invasor pode deixar uma mensagem junto com a nova "cara" que dá a pagina que fora vítima do ataque, quanto de autores, meios, modos, e eventual responsabilização dos administradores dos sistemas violados.

De fato, o que os dados mais elementares a respeito das desfigurações no mundo revelam é que mas de 50% destes ataques se dão ou devido a erro de configuração dos administradores de sistemas, ou por meio de falhas notórias existentes nos sistemas utilizados (Zone-H, 2004). Em alguns casos, os administradores efetivamente não cumprem suas funções (NOONAN, 2002), em outros são as empresas que fazem a escolha de não investir em sistemas de segurança até que sejam vítimas de ataques pela primeira vez, assumindo, de certa forma, o risco de expor os dados de seus clientes a hackers invasores.

Este tipo de realidade encontrada hoje não só no Brasil como no mundo, coloca o debate da criminalização da conduta isolada de invadir um sistema eletrônico. A criminalização desta conduta tem uma origem histórica muito pontual e razões bem claras, vinculadas aos meios de comunicação de massas nos Estados Unidos (HOLLINGER e LANZA-KADUCE, 1988). Não se entrará em detalhes, mas, ocorre que, depois de quase 15 anos mantendo uma política de punir criminalmente, com duras penas, essa conduta, o próprio governo estadounidense se manifesta no sentido de rever sua posição original e de permitir o chamado "hacking white hat" que seria o cometimento da invasão para fins de melhora dos sistemas de seguranças, atuando-se portanto em prol da sociedade (ANANOVA, 2002).

No caso do PL 84/99, se está atuando contra esta tendência, criminalizando o acesso indevido a sistema informatizado independente da natureza deste acesso. Seja ele em prol do interesse da sociedade ou contra ele, em nosso ordenamento jurídico ele será considerado crime e deverá ser combatido como tal.

Se levarmos em conta teorias criminológicas como a do etiquetamento, e o fato de os hackers constituirem-se em redes de relações sociais. Não seria difícil deduzir que com a criminalização, existe uma possibilidade significativa, de a rede de hackers invasores começar a estabelecer vínculos com redes do crime organizado (CRIMINAL ANALYSIS BRANCH, 2001), a exemplo do que ocorreu na Ucrânia e na Russia (SAVONA, 1998; SALKEVER, 2001) e do que se revela como atual tendência mundial (WILLIAMS, 2001), apesar de esta dedução se basear em aspectos teóricos e de não haver indicação empírica de que isso já ocorra enquanto fato social no Brasil.

5. SOCIOLOGIA DE REDES: UMA POSSIBILIDADE DE INTERVENÇÃO SOCIAL

Aqui há a preocupação de propor novas possibilidades uma vez que os meios atualmente empregados em outros países do mundo não parecem ter a eficácia desejada, ao ponto de alguns agentes de aplicação da lei efetivamente anunciam a perda da luta pela prevenção do cibercrime (HEGEL, 2002).

Como já discutimos anteriormente, a eliminação total de uma rede é uma tarefa difícil. Além do fato de que uma rede pode se interconectar com outras redes sempre que seus interesses sejam coincidentes.

Ao se continuar com o desdobramento da teoria de redes sociais, aplicando-a ao contexto brasileiro da rede de hackers invasores, ver-se-á que é possível propor um meio de combate ao crime de invasão de tal forma que não se busque a eliminação da rede, pura e simplesmente, mas sim, o uso da própria lógica de rede para criar uma rede paralela, adequada ao ordenamento jurídico pátrio, e que, absorva os nós da rede criminosa de modo a, pelo menos, reduzir-la tanto em seu tamanho quanto em sua capacidade lesiva.

Tal via surge do fato de que é possível inserir uma alteração no código da rede social de que tratamos de modo a alterar seu objetivo. Em termos práticos, isto corresponderia a, mediante intervenção de entes estatais, fazer com que as atividades desenvolvidas pela comunidade dos hackers invasores fossem convertidas em atividades de interesse da sociedade, idéia essa, de aproveitar o capital humano, que já fora apresentada em outros países com outros contextos (MEHTA, 2001) e que

se torna mais viável se levarmos em conta os próprios elementos da sub-cultura hacker, os quais, por sí só, não aparentam tender a delinqüência, mas sim a desviação.

Isso poderia ser possível se fosse permitido aos membros desta comunidade de hackers invasores um meio de atuarem como "hackers white hat" ou "hackers éticos"[9] em troca de reconhecimento social. Implicaria em se estruturar um serviço que, por um lado, desse a segurança jurídica ao hacker invasor para que esse faça suas tentativas de invasão, sendo que, se ocorrer de ser bem sucedido, se comprometa a informar a um intermediário, no caso a autoridade do estado, eventuais falhas de segurança em sistemas, de modo que essas informações fossem repassadas aos órgãos ou empresas cujo sistema seja falho. Por outro lado, tal serviço teria de dar garantias aos possíveis alvos desses "ataques éticos", obrigando esses hackers a manter em sigilo o nome dos órgãos ou empresas cujo acesso fora bem sucedido, a amplitude das falhas e os meios de entrada.

Por fim, o que se pleiteia é: evitar uma perda de capital humano altamente capacitado para redes do crime organizado; uma economia de recursos públicos, os quais poderiam se centrar em delinqüência eletrônica que ofereça risco efetivo à sociedade; e melhorar a atuação dos desenvolvedores e dos administradores de sistemas mediante constante controle social e estatal da qualidade dos mesmos.

6. REFERÊNCIA BIBLIOGRÁFICAS

ANANOVA, "Bush adviser promotes 'responsible hacking'" in Ananova News, 1st August, 2002.

CASTELLS, Manuel. "La Sociedad Red. Un Marco Analítico" in CASTELLS, Manuel, GIDDENS, Anthony e TOURAINE, Alain. *Teorias para una nueva sociedad*, Madrid: Fundación Marcelino Botin, 2003.

CRIMINAL ANALYSIS BRANCH, Criminal Intelligence Directorate. "Hackers: a Canadian police perspective - Part II" Royal Canadian Mounted Police, 30, May, 2001.

GIL, Gilberto, Discurso de abertura dos trabalhos da Semana de Software Livre no Legislativo, Brasília. 2003.

HEGEL, Rolf apud REUTERS. "Europe police losing cyber fight" in *MSNBC News*, 2002.

HIMANEN Pekka, TORVALDS, Linus e CASTELLS, Manuel. *The Hacker Ethic and the Spirit of the Information Age*. New York: Random House, 2001.

HOLLINGER, Richard C. e LANZA-KADUCE, Lonn. ``The Process of Criminalization: The Case of Computer Crime Laws," Criminology, Vol. 26, No. 1, 1988, p. 101-126

IEWGITC - Interpol European Working Group on Information Technology Crime, "White Hat v. Black Hat" in *SC Infosec Opinionwire*, December 11, 2002.

JORDAN, Tim e TAYLOR, Paul. *A Sociology of Hackers* in Sociological-Review; 46, 4, Nov, 757-780. Inglaterra: 1998

KELLERMANN, Tom apud VERTON, Dan. "Hacking syndicates threaten banking" in *ComputerWorld* November 4, 2002.

LEVY, Steven. *Hackers: heroes of the computer revolution*, USA: Penguin, 2001.

MEHTA, Dewang apud BBC. "Teen hackers turn cyber cops" in *BBC News South Asia*, January 3. 2001.

MEYER, Gordon R. *The Social Organization of the Computer Underground*, Thesis Northern Illinois University: Dept. of

MI2G, "Brazil exports Cyber-crime worldwide" in *News Release*: London, 18, November, 2002.

NISCC, *NISCC Monthily Bulletin*, July 2002.

NOONAN, Robert apud UPI, United Press International. "Pentagon computers tougher for hackers" in UPI News Update, International Desk, 29 de Outubro, 8:54 AM, 2002.

OxEn TRSh, Entrevista feita por Ariel G. Foina com representante do grupo Russo OxEn TRSh: Novembro 2002.

RAYMOND, Eric S. *The New Hacker's Dictionary*, Cambridge: MIT Press, 1996.

SALKEVER, Alex, "A World Wide Web of Organized Crime" in BussinesWeek On-Line, march 13, 2001

SAVONA, Ernesto U. (in collaborazione con federico lasco, andrea di nicola e paola zoffi). *Processi di Globalizzazione e Criminalità Organizzata Transnazionale*, Research Group on Transnacional Crime, University of Trento, Nº 29, Napoli, Italia, diciembre, 1998.

SILVA NETO, Amaro Moraes e, *O spam e o direito brasileiro (uma visão geral)*, São Paulo, inverno. 2002 (Apresentado ao Congresso Internacional De Direito E Tecnologias Da Informação, Brasília. 3 de Outubro de 2002).

SMITH, Tomy. "Brazil Becomes a Cybercrime Lab" in *New York Times*, October 27, 2003

STALLMAN, Richar. "On Hacking" in *Richard Stallman's home page*. 2002.

VATIS, Michael A, *Statement for the Record of Michael A. Vatis Director, National Infrastucture Protection Center, Federal Bureau of Investigation on NIPC Cyber Threat Assessment, October 1999 Before the Senate Judiciary Committee, Subcommittee on Technology and Terrorism*: FBI, Washington, 1999.

WILLIAMS, Phil. "Organized Crime and Cybercrime: Synergies, Trends, and Responses" in *Global Issues*: United States Department of State, August 2001, Vol.6, No 2, 2001.

ZONE-H. Strats and Graphs. In *Zone-h.Org*. 2004.

9 Ambos os termos se referem a um tipo de conduta de tentar invasões de acordo com princípios éticos de modo a não causar dano aos sistemas, relatando as falhas encontradas aos responsáveis para que os mesmos tenham a oportunidade de melhorar a segurança dos respectivos sistemas, protegendo-os assim de hackers invasores com intenções criminosas, designados pelo termo "hackers black hat".

GUERRA NA PAZ
AÇÕES MALICIOSAS SOBRE REDES E SISTEMAS DE INFORMAÇÕES

Frank Ned Santa Cruz de Oliveira
Pesquisador independente

Abstract

As computer networks and informational systems has become vital to institutions: academicals, commercial and governmental, becoming communication vehicles between those and the society, we became aware of the infrastructure exposure to malicious individuals. Therefore, it is necessary a deeper understanding of this phenomenon so the strategic and tactical plans of combat to these malicious actions can be established.

1. INTRODUÇÃO

Nos dias atuais, de entrechoques de civilizações num mundo globalizado e fragmentado, mais do que nunca se faz necessário interpretar os sinais da era vivida e ser capaz de reconhecer como a conjuntura internacional evoluiu. Ademais, saber quais as prováveis tendências do porvir, bem como, concomitantemente buscando determinar os interesses nacionais para definir o que e como fazer – a política e as estratégias a adotar.

Destarte, torna-se fundamental desenvolver uma visão estratégica global dos acontecimentos mundiais para ajudar na reavaliação dos meios e dos valores empregados, ao pesar as decisões tomadas, os métodos usados e as realizações obtidas.

A estratégia não deve ser uma doutrina única, mas um método de pensamento, permitindo classificar e hierarquizar acontecimentos e, depois, escolher os procedimentos mais eficazes. A cada situação corresponde uma estratégia particular; toda estratégia pode ser a melhor em uma das conjunturas possíveis e detestável em outras conjunturas.

Hodiernamente, a guerra tornou-se abertamente total, isto é, conduzida simultaneamente em todos os domínios, político, econômico, diplomático e militar.

Nesse contexto configura-se uma nova realidade com o surgimento da *netwar* que se trata do equivalente ao termo militar *cyberwar*.

Sendo assim, torna-se fundamental o desenvolvimento de ações estratégicas e táticas no sentido de atuar com respostas apropriadas, bem como o desenvolvimento de programas de cooperação entre instituições e atores deste novo cenário.

Assim o assunto abordado neste texto tem por objetivo principal tratar a *netwar* no aspécto da sociedade civil, desenvolvendo uma analogia de conceitos estratégicos empregados no universo militares e aplicáveis à segurança de redes e sistemas de informação. Com sua modesta abrangência, este trabalho pretende servir como motivação ao leitor para busca de novos conhecimentos. Não houve aqui a pretensão de esgotar o assunto, mas sim fornecer ao leitor um texto condensado, reunindo conceitos fundamentais ao entendimento dos termos relacionados, promove-los e coloca-los no centro de debate das questões estratégicas para instituições, governamentais, educacionais, privadas e por que não do Brasil. Várias obras serviram de apoio na elaboração deste material, as quais encontram-se elencadas ao final.

2. VISÃO GLOBAL DE ESTRATÉGIA

Estratégia, noção nascida da arte militar, estendendo-se atualmente a toda atividade humana.

Mas, o que é a estratégia?

Caso se parta da noção de estratégia militar, o ilustre autor, Carl Von Clausewitz definiu-a "como a arte de empregar as forças militares para atingir resultados fixados pela política". Já o general André Beaufre, resume a evolução do conceito: "a arte de promover o concurso de forças para atingir

os objetivos da política (...). É, por conseguinte, a arte da dialética de forças ou ainda, mais exatamente. A arte da dialética de vontades, empregando a força para resolver conflitos."

Tomando-se a definição de Aurélio Buarque, temos: "... 2. Arte de aplicar os meios disponíveis ou explorar condições favoráveis com vista a objetivos específicos."

Desta forma, as definições apresentada anteriormente nos ajuda a compreender a finalidade da estratégia: atingir os objetivos fixados pela política, utilizando da melhor maneira os meios de que se dispões. Esses objetivos podem ser ofensivos ou **defensivos**.

Adotando esses conceitos para segurança de redes e sistemas de informação, em uma nação que não esteja em estado de guerra, conforme definição comumente aceita, o principal objetivo é **defensivo** empregando-se uma estratégia de **dissuasão**.

O entendimento dos meios da estratégia permite melhor colocar em evidência a forma de raciocínio que lhe é própria.

Para atingir a decisão, a estratégia vai dispor de uma gama de meios materiais e morais, indo da implementação de tecnologias, estabelecimento de parcerias à divulgação de conceitos. A arte consistirá em escolher entre os meios disponíveis, e em combinar sua ação, para fazê-los convergirem para um mesmo resultado.

A escolha dos meios vai depender de uma confrontação entre as vulnerabilidades conhecidas e as possibilidades. Para fazer isso, é preciso analisar o efeito. O que se quer convencer? Em última analise, é o inimigo que se quer convencer. Para tanto deve-se definir uma ação direta ou **indireta**.

Na estratégia da ação indireta, o adversário não é derrotado, mas é vencido pela manobra, procura-se desgastá-lo progressivamente.

3. GUERRA

A guerra é uma forma de fazer política, ou pelo menos um meio de fazer política, já que, na verdade a guerra é a luta pelo poder. Guerra é o estado em que vivem aqueles que lutam. Na guerra ambos os lados buscam impor sua vontade. Destarte, a guerra é um fenômeno muito mais abrangente que o conflito armado. Guerra só existe se houver choque de vontades, tem que haver uma dialética de vontades.

Até o século XVIII, era claro como a guerra se processava: a guerra ocorria entre dois ou mais estados nacionais, representados por duas ou mais casas reais e normalmente era conduzida através de exércitos de mercenários. Hoje, não se pode prever com certeza como se dará uma guerra em um determinado espaço e em um dado tempo. Há, hoje, quatro diferentes tipos de guerra:

A guerra convencional;

A guerra de destruição em massa;

A guerra irregular; e

A guerra assimétrica.

A guerra irregular foi progressivamente tomando o lugar das guerras convencionais e caracteriza-se pela transferência dos conflitos para as ruas, cavernas, florestas e redes de computadores.

A guerra assimétrica é uma guerra irregular travada no espaço mundial e é composta, entre outras, das seguintes assimetrias:

Assimetria de poder econômico e financeiro – muitos recursos versus poucos;

Assimetria de estrutura organizacional - hierarquia versus rede;

Assimetria de objetivos – infinitos alvos versus poucos;

Assimetria de resultados – indiferença de resultados no curto e médio prazo contra a necessidade de resultados expressivos do adversário no curto prazo;

Assimetria comportamental – não sujeito a nenhuma regra, inclusive admitindo o suicídio na ação versus o adversário preso a regras e a convenções.

A guerra assimétrica, assim como a guerra irregular, é, devido a sua natureza, a guerra dos fracos contra os fortes, a guerra dos pobres contra os ricos. Ambas são fundamentalmente guerras de desgaste. Tanto a guerra assimétrica como a guerra irregular não é apenas guerra nas sombras, elas são **guerra na paz**, a guerra assimétrica é uma guerra que não se combate e, sim, se vive. A guerra assimétrica coloca-se como um tipo de guerra praticada pela estratégia de ação indireta. A guerra

irregular é a guerra do espaço amplo. A guerra assimétrica é a guerra do espaço ilimitado. Em ambas, não existem frentes de combate. A retaguarda não existe para elas. O espaço não é mantido, nem ocupado. O espaço é contaminado. São guerras de movimento.

Um dos principais movimentos é o da infiltração, que é característica central tanto operacional como tática. Podemos observar dois momentos principais: o de reunir e o de dispersar.

Sabemos que toda arma tem um alvo adequado. A guerra assimétrica não oferece alvos a um dos lados e oferece qualquer oportunidade como alvo ao outro. Em função disso, em um dos lados há muita dificuldade no emprego de determinados recursos enquanto no outro há ampla possibilidade de se empregar qualquer facilidade.

As formas de guerra assimétrica são:
Guerra psicológica;
Guerra econômica;
Guerra com armamento usual;
Guerra radiológica, nuclear ou radioativa;
Guerra biológica, bacteriológica ou virótica;
Guerra química;
Guerra cibernética, eletrônica ou informática.

Neste ponto voltamos nossa atenção para a *netwar*.

4. ASPÉCTOS DA NETWAR

A *netware* trata-se do equivalente ao termo militar *cyberwar*. *Netwar* possui uma natureza dupla, de um lado temos terroristas, criminosos e extremistas nacionalistas, já do outro lado temos o ativismo da sociedade civil. O que caracteriza a *netwar* como uma forma de conflito é a natureza da estrutura organizacional dos participantes que estão interconectados através das redes computacionais.

Trata-se de vários grupos, sem uma liderança definida, acefalarquias, que se organizam de forma extremamente rápida com o propósito de lançar ataques contra alvos /computacionais/eletrônicos de instituições comerciais, financeiras, educacionais e governamentais. Ataques estes que possuem natureza assimétrica e que não são limitados pelo átomo como os conflitos de épocas anteriores. Independente de quem sejam os protagonistas ativistas da sociedade civil ou terrorista, os ataques praticados com freqüência são bem sucedidos. Em parte o sucesso dos ataques praticados na *netwar* pode se explicado em função da novidade, ou seja, decorrente da exploração de novas vulnerabilidades para as quais não existem correções ou não houve tempo hábil para aplicar a correção, por outro lado a desinformação quanto à necessidade de mecanismos de segurança, de arquiteturas de redes seguras, procedimentos de resposta a incidentes, entre outros facilitam a ação do inimigo.

Outra característica marcante da *netware* é que além de ser uma guerra assimétrica, a origem dos ataques também é assimétrica o que dificulta em muito as ações de combate principalmente em virtude dos aspéctos legais.

Na *netwar* acontece o rompimento da mais velha convenção: a guerra como assunto exclusivo dos militares, em que se faz o emprego exclusivo de armas militares. A *netwar* não é conduzida exclusivamente por militares e não usa armamento militar. Há uma relação dialética entre a guerra assimétrica com origem assimétrica e a lei. Pois aquela pode apresentar uma manifestação de tendência revolucionária, ser ilegal, mas não necessariamente ilegítima. Não é possível ao agente operar de forma legal politicamente e de forma ilegal enquanto agente. O agente é totalmente ilegal. Acontece que o agente é ilegal perante uma legislação nacional, mas será que também o é perante a legislação internacional?

Nesta guerra os agentes constituem ou não redes, que se opõem a estruturas hierárquicas. A ligação entre agentes se dá muito mais horizontalmente em redes, pela fórmula política ou no plano das idéias, do que verticalmente, como resultado de estruturas de comando. A primazia que os agentes têm no estabelecimento de sistemas de redes sempre redunda em vantagens estratégicas e táticas. A multiplicação das redes gera do lado dos agentes, sistemas de heterarquias, panarquias e acefalarquias, todos incompatíveis com sistemas usuais de condução da guerra baseados em hierarquia. O soldado

está preso às convenções da guerra e o agente está livre de tudo, que não as regras de sua luta. Eles tornam-se neutros e desaparecem no campo de batalha.

A liberdade para operar neste tipo de guerra constrói a sua própria força. Liberdade vista aqui como liberdade sobre o espaço e sobre o tempo. Além da facilidade e velocidade que os agentes dispõem para rapidamente agruparem-se para lançar ataques. A forma de organização em redes computacionais permite a utilização de antigas formas de atividades ilícitas e lícitas. Em questões de minutos novas ferramentas de ataque são compartilhadas entre diversos grupos de forma mundial.

Na *netwar* existem cinco aspéctos que devem ser observados:

Tecnológico;

Social;

Narrativo;

Organizacional;

Doutrinário.

Embora o nível de sofisticação tecnológico faça diferença e em geral as pessoas pensem que se trata do principal aspécto, os demais níveis são de igual importância. Por exemplo, o nível social que caracteriza a cooperação entre os membros dos grupos. Embora os laços sociais sejam fortes, permitindo a construção de confiança mútua e identificação de valores, a forma de organização permite através da narrativa captar novos agentes para a causa .

A organização estrutural varia de canais diretos a estruturas de maior complexidade, como estrela dispersa por diversos paises. No passado, as ações de inteligência tinham foco em mapear a estrutura de hierarquia dos líderes na organização em rede, esta abordagem não é suficiente.

Com os avanços tecnológicos e facilidade de acesso às novas tecnologias o poder de comunicação, organização e ataque destes grupos vai aumentar de forma exponencial. Alguns exemplos são: comunicação criptografada, rede sem fio, a telefonia celular com IP (GSM), VoIP, *homing* de IP, *bluetooth*.

5. SISTEMA DE DEFESA EM CAMADAS MÚLTIPLAS

Faz-se necessária a elaboração de uma "Política de Defesa" bem como das diretrizes com a finalidade de empregarmos as estratégias e táticas adequadas. Para tanto alguns pontos fundamentais devem ser claramente explorados:

Quem são os ofensores?

Onde situam-se e com que grau de ameaça?

Quais são as vulnerabilidades?

Onde fortalecer e com que prioridade e intensidade?

Uma visão, em camadas, dos ativos a serem protegidos auxilia na elaboração das estratégias e táticas de contramedida. Uma abordagem é a segurança de perímetro alinhada com segurança em profundidade, *hardening*, tendo foco nos sistemas classificados de alta criticidade, núcleo, e vigilância dos sistemas periféricos.

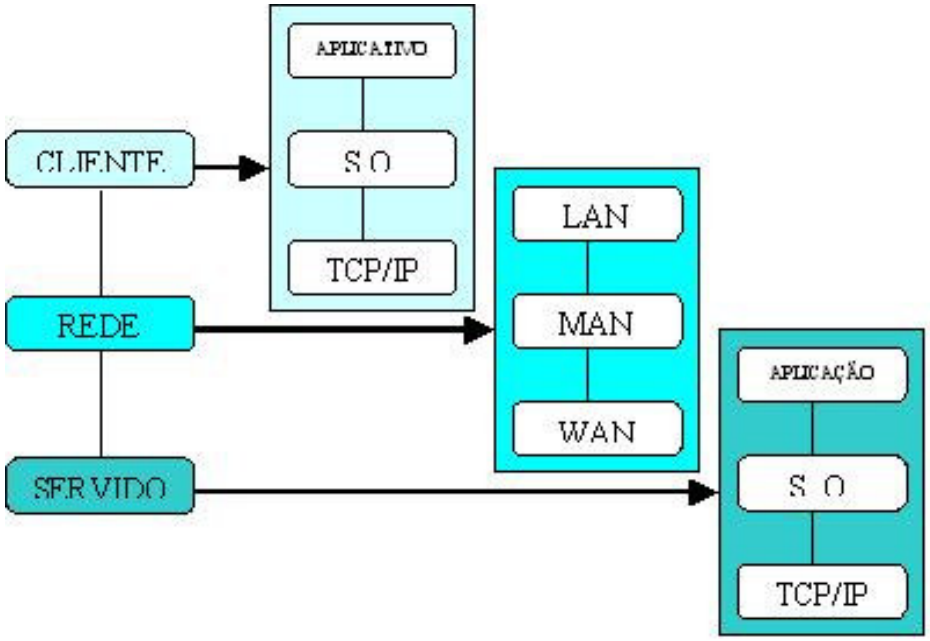


Figura 1 – Visão em camadas

Pode-se expandir o nível de detalhamento de cada uma das camadas até atingir a profundidade desejável. Por exemplo:

rede::WAN
Borda
Core
Distribuição
Acesso

Assim, tem-se uma visão em maior profundidade que auxilia a responder as questões fundamentais, no nosso exemplo:

Quem são os ofensores? *Crackers*, criminosos e vândalos.

Onde se situam e com que grau de ameaça? Situam-se externa a internamente, com diferentes graus de ameaça, conforme o ofensor.

Quais são as vulnerabilidades? Vulnerabilidades de arquitetura, sistemas operacionais, pilha TCP/IP e aplicações.

Onde fortalecer e com que prioridade e intensidade? Fortalecer os sistemas de núcleo de forma prioritária com a implantação de mecanismos de controle de conexão e segurança em profundidade.

É desejável que todos os mecanimsos possuam recursos de gerar registro dos eventos, *logs*, com o objetivo de serem centralizados e correlacionados em um Centro de Operações de Segurança, para finalidade de correlacionamento, análise forense, mineração de dados, possibilitando desta forma o efetivo acompanhamento de acordo com o C4I2 (Comando, Controle, Comunicação, Computador, Informação e Inteligência), que permite ações estratégicas, operacionais e táticas em tempo real permitindo a tomada de decisão em função da visão global dos eventos.

6. CONSIDERAÇÕES FINAIS

Sendo assim, faz-se necessária um amadurecimento perante a nova realidade, a definição de um plano estratégico de operações de "combate" que deve incluir a caracterização dos objetivos do inimigo, técnicas operacionais, recursos utilizados e agentes. Outrossim deve-se identificar as ações de combate legal e operacional, além de aparelhar os centros de gerência de segurança com tecnologia que permita a coleta e correlacionamento dos diversos eventos, permitindo desta forma uma visão global do teatro de operações e estabelecimento de parcerias com outros centros de segurança."

A defesa tem uma finalidade passiva: preservação; o ataque, uma positiva: conquista. Este aumenta nossa capacidade de condução da guerra, aquela não" (Carl Von Clausewitz)

7. REFERÊNCIAS BIBLIOGRÁFICAS

BEAUFRE, André. Introduction a la Stratégie; TRADUÇÃO DE Luiz de Alencar Araripe (Biblioteca do Exército).
CLAUSEWITZ, Carl Von. Da Guerra; TRADUÇÃO DE Maria Teresa Ramos (Martins Fontes).
CARDOSO, Alberto Mendes; Os Treze Momentos – Análise da Obra de SUN TZU (Biblioteca do Exército).
STEPHESON, Peter; Investigating Computer-Related Crime (CRC).
MACHIAVELLI, Niccolo; O Príncipe – COMENTÁRIOS DE Napoleão Bonaparte (Biblioteca do Exército).
PARET, Peter; Construtores da Estratégia Moderna (Biblioteca do Exército).
ARQUILLA, John / RONFELDT, David; In Athena´s Camp (RAND).
FERREIRA,Aurélio Buarque de Holanda. Dicionário da Língua Portuguesa.
SANTOS, Murilo; Segurança Defensica – Ideais, Disponível em: <http://www.mct.gov.br/CEE/revista/Parcerias3/seg_def.html> Acesso em: 07 mai. 2004.
COSTA, Darc;.Visualizações da Guerra Assimétrica , Disponível em: <http://www.militar.com.br> Acesso em: 07 mai. 2004.

O SPAM A SERVIÇO DAS FRAUDES E GOLPES DIGITAIS

Renata Cicilini Teixeira

CPQD - Centro de Pesquisa e Desenvolvimento - Telecom & IT Solutions
Rod Campinas – Mogi-Mirim, km 118,5 – SP340 – CEP 13086-902 – Campinas/SP
renatat@cpqd.com.br

Abstract

The first spam e-mails were about chain letters, hoaxes and advertisement. Nowadays, spam e-mails carry computer viruses, trojans and all sorts of malware. Futhermore, spam e-mails can make use of social engineering techniques to convince users to open e-mails and a malicious link, applying scams and other kinds of frauds.

This paper discusses the evolution of spam, including techniques and types of spam. It illustrates how spam is used to increase on-line scams and frauds, compromise systems and network security, and cause losses to users and companies.

1. INTRODUÇÃO

O spam é a prática de enviar e-mails não solicitados, ou seja, é toda mensagem eletrônica enviada a um ou mais usuários, sem que estes tenham explicitamente solicitado o envio da mesma.

O primeiro spam registrado na história aconteceu em abril de 1994, quando um casal de advogados enviou uma mensagem contendo propaganda de uma loteria de *green card* americano para todos os grupos de discussão da USENET [7]. Desde então, a quantidade e diversidade de e-mails não solicitados têm aumentado e atingiu à assustadora cifra de 75% dos e-mails válidos veiculados na Internet em junho de 2004.

Os impactos do spam são muitos:

A chateação causada ao usuário final, além do prejuízo também.

Os prejuízos acumulados pelas empresas, que vêem parte do valioso tempo dos funcionários sendo gasto para limpar caixas postais.

A ameaça à viabilidade de utilização do e-mail como ferramenta de comunicação.

O comprometimento da segurança de rede.

Com relação à segurança da rede, trata-se de um aspecto fundamental, à medida que o spam tem sido vetor de propagação de vírus e outros códigos maliciosos, bem como veículo para a aplicação de golpes e fraudes. Ainda neste contexto, os vírus mais recentes permitem utilizar os sistemas contaminados como base para o envio de spam. Complementando, o mesmo ocorre com os sistemas invadidos em decorrência da exploração de vulnerabilidades de segurança.

Desta maneira, o spam deixou de ser uma mera chateação e inconveniência, tornando-se uma ameaça real à segurança da rede e à utilização segura da Internet como meio de comunicação e negócios.

2. OS TIPOS DE SPAM E SUA EVOLUÇÃO

Existem vários tipos de spam [2]. Depois do registro do primeiro spam [12], houve a disseminação das correntes, como por exemplo, aquelas que prometiam sorte e dinheiro a quem as repassasse e desgraça àqueles que não o fizessem.

Os boatos são outro tipo de spam que evoluiu por si só. Eles deixaram de incluir viagens gratuitas a *Disneyworld*, para contar histórias capazes de difamar produtos e empresas. As lendas urbanas são muito parecidas com os boatos, porém, são histórias mais sinistras e sempre têm aquele "tom" de verdade, dizendo que o fato aconteceu com alguém supostamente conhecido.

Os spams contendo propaganda de produtos e serviços são conhecidos como UCE, *Unsolicited Commercial E-mail*, constituem um caso a parte na discussão sobre o spam, pois envolvem as questões sobre o *marketing* legítimo por e-mail e as malas diretas, por exemplo. Esta discussão não faz parte do escopo deste artigo, porém vale lembrar que o primeiro registro spam foi um UCE [7].

Outros tipos de spam encontrados são as ameaças, os e-mails contendo pornografia, oferecendo produtos mirabolantes e inexistentes.

O próximo passo na evolução do spam foi decisivo para o aumento no volume de spam e também para a maior proliferação de vírus e códigos maliciosos. A união dos *spammers* (os que praticam o spam) e *coders* (os desenvolvedores de vírus) trouxe dois novos cenários preocupantes: o uso dos e-mails de spam como vetores de propagação dos códigos maliciosos e os vírus capazes de tornar o sistema infectado um emissor de spam. Com isto, houve um significativo aumento nas máquinas usadas para o envio de spam, dificultando cada vez mais a identificação da real origem do spam.

Continuando a análise, identifica-se uma das mais recentes utilidades do spam: a aplicação de golpes (*scams*) e fraudes. É importante ressaltar que podem existir vários tipos de fraudes e golpes na Internet, porém, no escopo deste artigo, são consideradas àqueles propagados por e-mail.

Este tipo de atividade ganhou adeptos após o desenvolvimento do comércio eletrônico e do *Internet Banking*. No Brasil e em outros países, houve um significativo aumento da quantidade de fraudes e golpes no último ano, o que pode ser justificado pelos seguintes motivos: o uso do spam como ferramenta de propagação e o aumento do número de denúncias, devido a uma maior conscientização do usuário.

A Figura 1 ilustra o aumento das fraudes na Internet brasileira, no período de janeiro de 2003 até junho de 2004, de acordo com as estatísticas computadas pelo NBSO, *NIC Br Security Office*, o grupo de resposta a incidentes de segurança ligado ao Comitê Gestor da Internet Br [3].

Analisando os números mostrados nota-se a discrepância registrada nos últimos meses de 2003, quando houve a maior proliferação deste tipo de atividade. Por outro lado, a diminuição registrada nos meses de abril a junho de 2004 podem estar refletindo a reação da comunidade de usuários, estando mais alerta com relação às fraudes, além da atuação dos grupos de resposta a incidentes de segurança das redes e empresas vítimas de fraude.

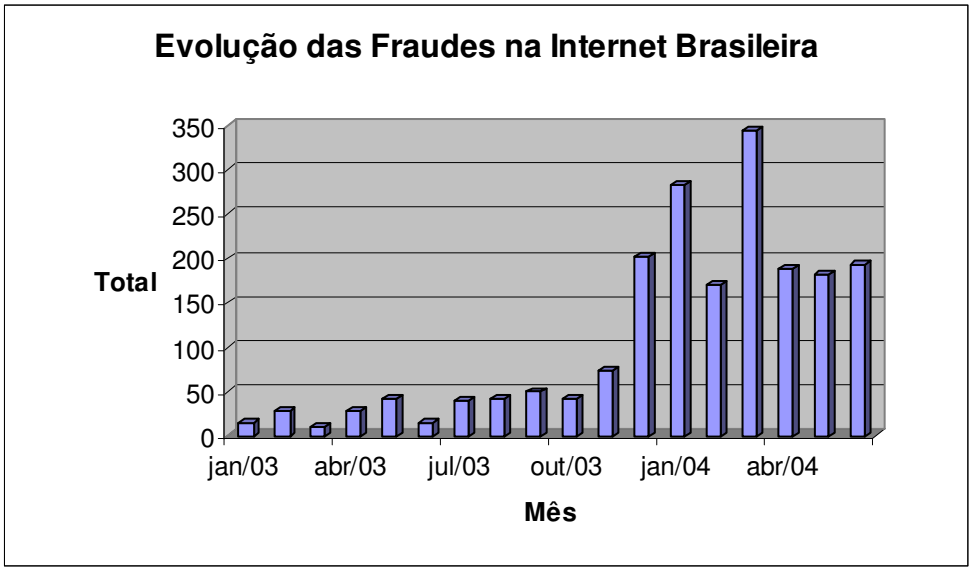


Figura 1 - Fraudes na Internet Brasileira (Fonte: NBSO)

Finalmente, os espécimes de spam detectados nos últimos meses são o SPIM, spam via *Instant Messenger*, e o spam via redes sociais. Em ambos os casos, têm-se mensagens não solicitadas sendo enviadas. O SPIM tem como alvo os usuários de aplicativos para troca de mensagens instantâneas, como o ICQ e o *Microsoft Messenger*, por exemplo. Já os usuários das redes sociais, como o *Orkut* [9] e *LinkedIn* [5], por exemplo, são atingidos por mensagens enviadas em massa para todos os usuários cadastrados.

Neste contexto, conclui-se que não só aumentou a quantidade de spam veiculada na rede, mas também a diversidade de tipos e usos desta prática.

2.1. Os Artifícios dos Spammers

Os spammers têm dois objetivos: o anonimato e garantir que suas mensagens sejam lidas. Para tanto, utilizam artifícios técnicos ou não, visando esconder sua identidade, falsificar a real origem dos e-mails enviados, burlar os filtros e convencer o usuário a abrir o e-mail de spam.

Os artifícios técnicos são:

O uso de sistemas comprometidos, através da exploração de vulnerabilidades. Tais sistemas, também chamados de zumbis, se tornam bases de ataque e podem ser utilizados para armazenar ferramentas hacker, disparar ataques dos mais variados tipos e enviar spam.

O uso de sistemas contaminados por vírus. A maioria dos vírus propagados no último ano possui características e funcionalidades que auxiliam na propagação de spam, como a capacidade de instalar SMTP *engines* nos sistemas comprometidos.

O uso de sistemas indevidamente configurados, como aqueles com *open-relay* e *open-proxy*.

O uso de força bruta (*brute force*) para validar endereços de e-mail de determinado domínio. Neste caso, ferramentas automatizadas enviam grande quantidade de e-mails a um domínio específico, gerando os endereços a partir de dicionários de nomes e e-mails comuns. Assim, é possível validar a base de e-mails, desconsiderando as respostas recebidas como "usuário desconhecido" (*user unknown*). Esta técnica pode resultar em um ataque de negação de serviço ao servidor do domínio alvo, dependendo do volume de e-mails enviados.

O uso do *harvesting* (colheita) de e-mails disponíveis na rede. Trata-se de ferramentas automatizadas, capazes de varrer a Internet, coletando endereços de e-mail. As fontes mais consultadas são: os *web sites*, os *Instant Messengers*, as redes sociais e os *chats*.

A falsificação dos campos dos cabeçalhos dos e-mails, o que dificulta bastante a identificação do spammer e da origem do e-mail.

Entre os artifícios não-técnicos, pode-se destacar:

O uso de técnicas de engenharia social, com o objetivo de convencer o usuário a abrir e até responder o e-mail. Vale lembrar que a resposta do usuário valida seu e-mail, incluindo-o definitivamente na base dos *spammers*.

A alteração dos *subjects* com o intuito de driblar os filtros anti-spam, como por exemplo: "v!@gra".

O uso de *subjects* vagos o suficiente ou atraentes o suficiente para convencer o usuário a abrir o e-mail. Alguns exemplos são: "seu CPF" e "renovação de senha".

As justificativas incluídas no e-mail de spam, na tentativa de legitimá-lo. Alguns exemplos são: "De acordo com a lei xxxx, este e-mail não pode ser considerado spam" e "Você foi indicado por um amigo e por isso estamos contatando-o".

3. AS FRAUDES E GOLPES NA INTERNET

As fraudes e golpes passaram do mundo real para o mundo virtual. Hoje é possível presenciar os golpes de ganho de dinheiro fácil, trabalhe em casa, emagreça sem sacrifício, antes enviados por carta às vítimas, agora chegam por e-mail. Da mesma forma, as fraudes bancárias, ocorridas através da

clonagem de cartões ou roubo de senhas, são feitas via e-mail, convencendo o usuário a fornecer sua senha em um formulário falso de recadastramento bancário.

Os tipos mais comuns de golpes e fraudes registrados na Internet são:

Os esquemas de ganho de dinheiro fácil, prometendo rendimentos espetaculares em prazos reduzidos. Geralmente, pedem algum tipo de contribuição financeira, a ser enviada ou depositada em conta bancária.

As oportunidades de negócio, oferecendo maneiras de ganhar dinheiro sem muito trabalho ou investimento. Também pedem alguma contribuição simbólica em dinheiro.

As promessas de melhora da saúde através de medicamentos espetaculares, capazes de emagrecer dormindo, por exemplo.

Os golpes da Nigéria, também chamados de *4-1-9 nigerian scams*, são golpes classificados com "antecipação de pagamentos". Há registros deste tipo de golpe desde 1980 por cartas. Agora, o golpe circula na Internet, oferecendo a fortuna de militares nigerianos ou de outros países africanos, em troca de um depósito inicial, por exemplo. Outra variante do golpe oferece comissões milionárias em troca de ajuda em transações financeiras do governo nigeriano, ou ainda, em obras irregulares na Nigéria.

A mendicância virtual é outro tipo de golpe que tem se proliferado na Internet. São e-mails contando a história de falências de empresas e pedindo ajuda financeira para recuperá-las ou ajudar aos falidos.

Os *phishing scams* talvez sejam o tipo mais grave de fraudes e golpes registrados. São e-mails que visam obter dados do usuário, tais como senhas bancárias e números de documentos. Os textos dos e-mails fraudulentos geralmente não são bem escritos, mas são escritos para convencer o usuário de que se trata de um comunicado oficial, usando recursos de engenharia social e incluindo os logotipos das empresas. Alguns exemplos são os diversos e-mails de bancos enviados, contendo endereços de sites falsos dos referidos bancos, solicitando o recadastramento de senhas bancárias ou então oferecendo produtos, ou ainda, os e-mails falsos da Receita Federal ou Polícia Federal solicitando o recadastramento de CPFs e CNPJs.

O *Anti-Phishing Working Group* [1] é uma associação dedicada a combater as fraudes e golpes realizados na Internet através das técnicas de *phishing*, que incluem principalmente o *e-mail spoofing* e o roubo de identidade. O relatório divulgado pelo referido grupo em maio de 2004 [10] revela que as fraudes e golpes via Internet são uma tendência mundial e tem tido como vítimas os clientes de bancos americanos, empresas de cartões de crédito internacionais e sistemas de pagamento on-line.

4. PREVENÇÃO E COMBATE ÀS FRAUDES E GOLPES POR E-MAIL

Ainda não existe solução definitiva para o spam, porém existem mecanismos capazes de minimizar seu impacto, tais como os filtros anti-spam, por exemplo, que podem ser utilizados nos servidores e nos clientes de e-mail.

Com relação às fraudes e golpes, o caminho da prevenção passa necessariamente pela definição e cumprimento de políticas de segurança e de uso aceitável; correta aplicação das leis vigentes para os crimes digitais; bem como da educação e conscientização do usuário para que siga as melhores práticas para o uso do e-mail, incluindo:

Seguir as normas e conselhos definidos na Netiqueta [11] para o uso do e-mail.

Utilizar um antivírus e mantê-lo sempre atualizado.

Não abrir e-mails com arquivos em anexo, sem antes executar um antivírus.

Ter cuidados ao navegar em sites divulgados por e-mails de procedência duvidosa.

No abrir páginas de bancos ou outras instituições financeiras, divulgadas por e-mail.

Ao configurar filtros anti-spam, ter os cuidados em formar uma white list com os endereços de e-mail de seus parentes, amigos, colaboradores e parceiros de negócio. Também é recomendado enviar uma mensagem avisando ao remetente, caso seu e-mail tenha sido barrado pelo filtro anti-spam.

5. CONCLUSÃO

Se não existisse o spam, talvez os golpistas e fraudadores tivessem encontrado outra maneira de chegar até o usuário da Internet. No entanto, com a ajuda do spam, a tarefa ficou bastante facilitada, como discutido no presente artigo.

Como a história mesmo demonstra, as atividades ilícitas e seus executores sempre existirão, enquanto a sociedade busca maneiras de se defender e também de punir os responsáveis. Na Internet, não é e nem será diferente.

Concluindo:

Cabe à comunidade de usuários da Internet, estar cada vez mais atenta aos riscos apresentados pelo mundo virtual, que não são diferentes daqueles do mundo real.

Cabe à comunidade de técnicos, acadêmicos, instituições de pesquisa e empresas, a busca por soluções técnicas que minimizem o impacto do spam e conseqüentemente, de seus diversos tipos.

Cabe à polícia estar cada vez mais preparada, inclusive tecnicamente, para apurar e autuar em casos de fraudes, golpes e outros crimes digitais.

Cabe aos órgãos da justiça, fazer cumprir as leis que punem tais atividades ilícitas, como os golpes e fraudes. Caso não existam leis aplicáveis, que o poder legislativo seja envolvido para que tais leis sejam criadas em tempo hábil para frear a proliferação dos danos e prejuízos causados por este tipo de atividade.

Cabe aos governos trabalhar por uma integração entre os países, de modo a interagir sobre investigações relacionadas ao spam e principalmente por acordos que garantam a punição ao spam, driblando o problema da territorialidade da legislação de cada país.

Desta maneira, o combate surge em várias frentes e deve contar com a colaboração de diversos segmentos. Só assim, será possível vislumbrar uma chance cada vez maior de derrotar o inimigo: o spam, que como visto neste artigo, também está a serviço das fraudes e golpes digitais.

6. REFERÊNCIAS

[1] Anti-Phishing Working Group: http://www.antiphishing.org/
[2] "Características e tipos de Spam", Renata Cicilini Teixeira.
http://informatica.terra.com.br/virusecia/spam/interna/0,,OI195557-EI2403,00.html
[3] Estatísticas do NBSO: http://www.nbso.nic.br/stats/
[4] "FTC Names Its Dirty Dozen: 12 Scams Most Likely to Arrive Via Bulk Email"
http://www.ftc.gov/bcp/conline/pubs/alerts/doznalrt.htm
[5] Linked In: http://www.linkedin.com/
[6] Movimento Anti-Spam Brasileiro: http://www.spambr.org
[7]"O Primeiro Spam", http://web.archive.org/web/20011214024742/math-www.uni-paderborn.de/~axel/BL/CS941211.txt
[8] "Origin of the term "spam" to mean net abuse"
http://www.templetons.com/brad/spamterm.html
[9] Orkut: http://www.orkut.com
[10] Phishing Attacks Trend Report May 2004, Anti-Phishing Working Group:
http://www.antiphishing.org/APWG_Phishing_Attack_Report-May2004.pdf
[11] RFC 1855 Netiquette Guidelines: http://www.faqs.org/rfcs/rfc1855.html
[12] "Uma década de spam", Renata Cicilini Teixeira,
http://www.infoguerra.com.br/infonews/viewnews.cgi?newsid1081411540,93939,

UMA ANÁLISE CRÍTICA SOBRE A SEGURANÇA DE REDES SEM FIO NA CIDADE DE SÃO PAULO

Adriano Mauro Cansian[1], André Ricardo Abed Grégio[1], Aleck Zander Tomé de Sousa[1,2], Antonio Montes Filho[3]

[1]UNESP – Universidade Estadual Paulista
[2]Instituto Nacional de Pesquisas Espaciais – INPE/MCT
[3]Centro de Pesquisas Renato Archer – CenPRA/MCT

{adriano,andre}@acmesecurity.org, aleck@lac.inpe.br, antonio.montes@cenpra.gov.br

Resumo

Este trabalho apresenta um estudo de caso contendo uma análise crítica sobre a situação atual da segurança de redes sem fio na cidade de São Paulo, Brasil. Este estudo quantitativo é utilizado como fundamento para descrever as principais vulnerabilidades e problemas de segurança existentes em uma rede de computadores sem fio, utilizando os protocolos do padrão 802.11.

1. INTRODUÇÃO

O decréscimo dos custos aliado ao desenvolvimento constante da tecnologia móvel, e de sua banda de passagem disponível, são fatores preponderantes na crescente utilização dos dispositivos de redes sem fio sob o padrão 802.11 [ANSI/IEEE 1999]. A aplicação destes dispositivos varia desde o acesso móvel à rede local até como meio de interconexão de pontos distantes (compartilhamento de saída única para a Internet).

No Brasil observa-se atualmente que esta tecnologia tem sido ainda pouco usada para proporcionar mobilidade a usuários. No entanto, estas redes têm servido principalmente como meio de interligação de filiais de empresas, para acesso à rede institucional ou para conexão com redes externas e a Internet.

É bem sabido que a diferença mais evidente destas redes em comparação às redes guiadas está na camada física, onde o cabeamento é substituído pela emissão de radiofreqüência em um meio não-guiado e aberto. Este fato gera uma preocupação ímpar com relação à segurança; os dados são suscetíveis a programas que monitoram ondas de rádio, influenciando assim em sua confidencialidade e integridade.

Este artigo trata das vulnerabilidades e problemas de segurança das redes sem fio atuais, apresentando uma análise quantitativa dos problemas de segurança encontrados na cidade de São Paulo. Por intermédio de um trabalho de campo minucioso, foram coletados diversos tipos de informações que ilustram como as redes sem fio estão desprotegidas, com o intuito de comprovar a ameaça real e imediata a que estão sujeitas tais redes. São apresentadas estatísticas e informações de casos reais, comprovando que a má configuração dos equipamentos de rede sem fio, ou mesmo o uso de configurações padronizadas ou *default* [Park and Dicoi 2003], são os originadores das situações de risco.

2. RISCOS DE ATAQUES A REDES SEM FIO

Os riscos de ataques e violações à segurança das redes sem fio podem ser divididos em dois grandes grupos: riscos de ataques de origem interna e riscos de ataques de origem externa [AirDefense 2002].

Dentre os riscos internos são predominantes as falhas de configuração da rede e de equipamentos. Este trabalho dedica particular atenção a este problema pois, segundo nosso entendimento, trata-se do fator de mais alto risco atualmente presente nas redes sem fio brasileiras. Um dos principais objetivos é mostrar que configurações ineficientes estão colocando em risco as redes sem fio e, consequentemente, as redes guiadas. No que tange aos riscos de ataques externos, esta pesquisa concentra-se na possibilidade de quebra de confidencialidade da rede, através da captura de dados e informações trafegadas no meio aberto.

3. PROCEDIMENTOS E PESQUISA DE CAMPO

A principal motivação para esta pesquisa é compreender a real situação de risco de segurança em que se encontram as redes sem fio nas cidades brasileiras. Uma vez que é crescente a aplicação destas redes nos mais diversos sistemas de informação críticos, nosso objetivo é alertar para a necessidade de proteção contra ataques, fraudes e outros crimes eletrônicos. A intenção é obter uma análise crítica e real das condições em que se encontram as redes sem fio em uma região de grande concentração de negócios e serviços, de tal forma que este estudo possa ser utilizado para a orientação da adoção de medidas de proteção adequadas.

Segundo nosso conhecimento, esta é a primeira vez que um estudo deste tipo é apresentado com este tratamento e abrangência.

3.1. Inspeção e sondagem

Esta pesquisa utiliza extensivamente procedimentos de inspeção e sondagem de redes sem fio, conhecidos popularmente por *war driving* [Peikari e Fogie 2002] - uma varredura em uma área geográfica em busca de redes sem fio e suas informações. Tal procedimento não constitui um ataque contra a rede em questão, pois os programas ou códigos utilizados simplesmente capturam informações que estão sendo divulgadas publicamente, de forma aberta através das ondas de rádio.

Existem várias ferramentas de software gratuitas disponíveis publicamente para busca e sondagem de redes sem fio. Estas ferramentas quando utilizadas de forma apropriada, fornecem diversas informações importantes, como por exemplo, Identificador da rede (SSID - *Service Set Identification*), endereço *MAC*, criptografia *WEP* [ANSI/IEEE 1999], canal em uso [IEEE 1999], potência do sinal.

3.2. Sondagem ativa e passiva

Duas técnicas podem ser empregadas para a descoberta de redes sem fio: a sondagem ativa e a sondagem ou monitoramento passivo [Wright 2002].

Na sondagem ativa há troca de informações entre o cliente e o concentrador de acesso (*access point*) sob sondagem, podendo inclusive haver violação de políticas de segurança ou até mesmo acionar eventuais detectores de intrusão.

O monitoramento passivo, ou RFMON [Wright 2002], consiste na captura de todos os sinais de radiofreqüência em canais pré-configurados. A interface de rede sem fio é colocada em modo monitor [Cansian et al. 2003], capturando apenas o tráfego de difusão pública, sendo incapaz de transmitir quaisquer *frames*.

Este trabalho utilizou exclusivamente sondagem passiva, com leitura apenas das informações de difusão públicas dos *beacon frames* [Arbaugh et al. 2001], sem captura de transmissão de dados de conexões entre clientes e servidores, nem troca ou inserção de informações entre a sondagem e o possível concentrador de acesso ou conexão emissora.

4. AMBIENTE DA PESQUISA DE CAMPO

O equipamento básico principal utilizado neste trabalho consiste de um computador portátil, tipo notebook, marca Toshiba com processador Pentium 4, 1.8 GHz, 256 MB de memória RAM, com o sistema operacional *Linux Slackware 9.1* (http://www.slackware.org) com versão de *kernel* 2.4.22 e

uma interface PCMCIA de rede sem fio Dell TrueMobile 802.11b com entrada para conector tipo *MC* para conexão com antena externa.

Foi utilizado o software de monitoramento *Kismet*, versão *feb.04.01*. Foi aplicado o *patch* http://airsnort.shmoo.com/orinocoinfo.html no driver Orinoco para operação em "modo monitor". Neste modo ele mantém a troca automática de canais, para que seja possível executar a varredura em todas as frequências. O *Kismet* é um analisador de tráfego de camada de enlace, com licença *GPL*, e atua como um detector de redes sem fio cujos protocolos sejam 802.11a, 802.11b ou 802.11g. Funciona com interfaces que suportem o monitoramento passivo.

A antena externa utilizada é um dispositivo para comunicação móvel com base magnética para fixação no teto de veículos, e possui 22 cm de altura e 1,50 m de cabo coaxial tipo RG174 com conector tipo MC na extremidade, para conexão à interface PCMCIA. A impedância é de 50 ohms e a freqüência nominal de operação é de 2400 a 2483 MHz com potência máxima de até 50 W. Possui ganho de 5,5 dBi (referente à especificação antes da atenuação do cabo), quando montada sobre uma superfície de metal de pelo menos 1 metro de diâmetro. A atenuação média do cabo utilizado é de 1,3 dB por metro. Portanto, o ganho da montagem utilizada é de aproximadamente 3,53 dB.

Para registro da movimentação e determinação da localização foi utilizado um dispositivo de GPS (*Global Positioning System*) da marca Garmin modelo Etrex Vista, o qual se comunica com o computador portátil por intermédio de um cabo serial em conjunto com o software *GPSd* para sistema operacional Linux (http://pygps.org/gpsd/downloads/gpsd-1.07.tar.gz).

Por fim, para o traçado dos mapas das regiões pesquisadas, foi desenvolvido um *script* em *perl*, que converte os dados armazenados pelo *Kismet* (em formato XML) para o formato reconhecido pelo software *GPS Track Maker* (http://www.gpstm.com), sob sistema operacional Microsoft Windows.

5. REGIÃO PESQUISADA E METODOLOGIA APLICADA

A coleta de dados desta pesquisa optou por analisar algumas áreas específicas com grande concentração de empresas de negócios e serviços, notadamente bancos, corretoras, seguradoras, escritórios de representação, hospitais, clínicas, e estabelecimentos comerciais diversos, além de outros tipos variados de instituições. As duas áreas inicialmente pesquisadas na cidade de São Paulo foram as regiões da Avenida Paulista e da Avenida Luiz Carlos Berrini, e as suas imediações. Estas duas áreas englobam praticamente o centro financeiro do Brasil, e a maior concentração das empresas de alta tecnologia da cidade de São Paulo. Também foram realizadas pesquisas através dos eixos principais que unem estas duas regiões, notadamente na região da Avenida Juscelino Kubitschek e na região da Avenida Brigadeiro Luiz Antonio.

Foram realizadas quatro leituras e coletas de dados entre os dias 25 de fevereiro e 08 de março de 2004, todos em dias úteis. Cada leitura engloba as 3 regiões pesquisadas. Todas as leituras foram realizadas entre 14:00 e 15:30 (GMT-03) e tiveram duração média eficaz de 1h22m cada uma. O horário e o tempo de leitura foi padronizado, para manter condições semelhantes em cada pesquisa. O percurso total pesquisado em cada leitura foi de 30.47 Km.

6. RESULTADOS

Dentro de toda a área pesquisada, considerando a interpolação dos 4 dias de medidas realizadas, foram encontradas várias redes compatíveis, entre concentradores de acesso, redes *AD-HOC* (comunicação direta entre computadores, sem o uso de um concentrador de acesso) e *radio-bridges* para interconexão de redes. A Tabela 1 a seguir ilustra a distribuição destas redes nas 3 grandes áreas pesquisadas, e mostra a quantidade de redes que utilizam protocolo criptográfico *WEP* e as que não utilizam.

Tabela 1. Distribuição da quantidade de redes sem fio padrão 802.11b encontradas por região, relacionadas com o uso ou não de protocolo criptográfico *WEP*.

Região	Redes com *WEP*		Redes sem *WEP*		**TOTAL**	
	Quant.	%	Quant.	%	Quant.	%

Av. Paulista e imediações:	26	8.23	89	28.16	115	36.39
Av. Berrini e imediações:	56	17.72	74	23.42	130	41.14
Eixo Juscelino / Brigadeiro:	22	6.96	49	15.51	71	22.47
TOTAL:	104	32.91	212	67.09	316	100

Do total geral de 316 redes sem fio encontradas, foi registrado que 212 delas não estavam usando o protocolo de criptografia *WEP*, representando assim 67.09% do total de redes apuradas nas áreas pesquisadas.

Outra informação relevante obtida é que considerando o total de redes encontradas, 32 delas estavam com a configuração *default* do fabricante, ou com somente uma pequena modificação de troca do canal de comunicação utilizado. Isto representa 10.13% do total de redes encontradas nas regiões pesquisadas.

As figuras mostram as representações das redes encontradas, de acordo com a localização geográfica aproximada das posições onde o sinal foi detectado. Os esquemas classificam as redes quanto ao o uso de criptografia *WEP* (pontos escuros) ou não (pontos claros).

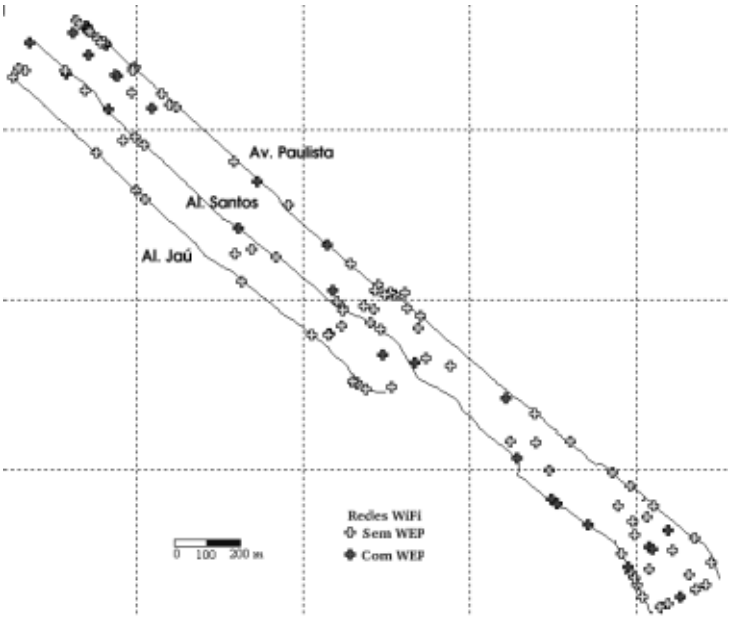


Figura 1. Distribuição das redes na região da Av. Paulista e imediações. As marcas claras representam a detecção de redes com ausência de criptografia. Nesta região concentram-se 28.16% de redes sem criptografia, considerando-se o total de redes da pesquisa. Considerando-se apenas as redes encontradas nesta região, as redes sem criptografia representam 77.4% do total desta área.

Apesar da pesquisa coletar as coordenadas geodésicas por intermédio de sistema de GPS, estes dados não são apresentados aqui, para preservar as informações sobre as redes. Pelo mesmo motivo, as figuras não apresentam as ruas e cruzamentos exatos das regiões pesquisadas. Optou-se por identificar apenas alguns pontos de referência, para ilustrar a distribuição dos pontos detectados por região.

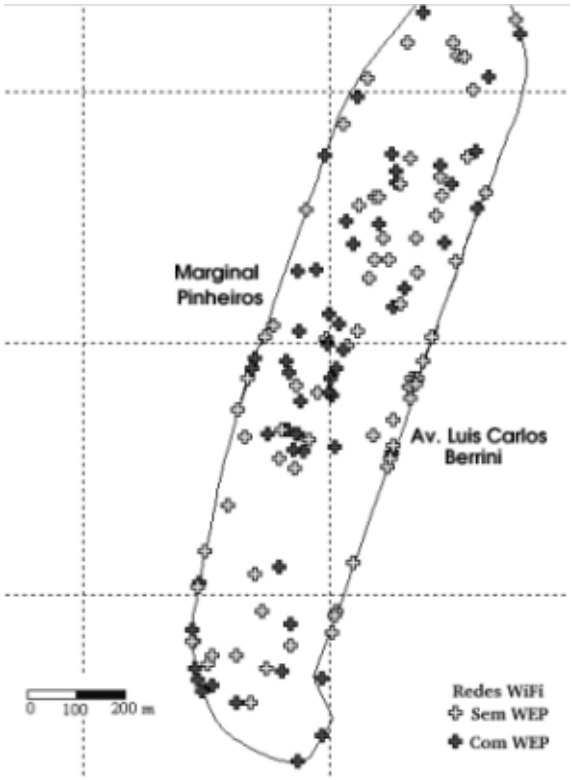


Figura 2. Distribuição das redes na região da Av. Engenheiro Luis Carlos Berrini e imediações da Marginal de Pinheiros. As marcas claras representam a detecção de redes com ausência de criptografia. Nesta região concentram-se 23.42% de redes sem criptografia, considerando-se o total de redes da pesquisa. Considerando-se apenas as redes encontradas nesta região, as redes sem criptografia somam 56.9% do total desta área.

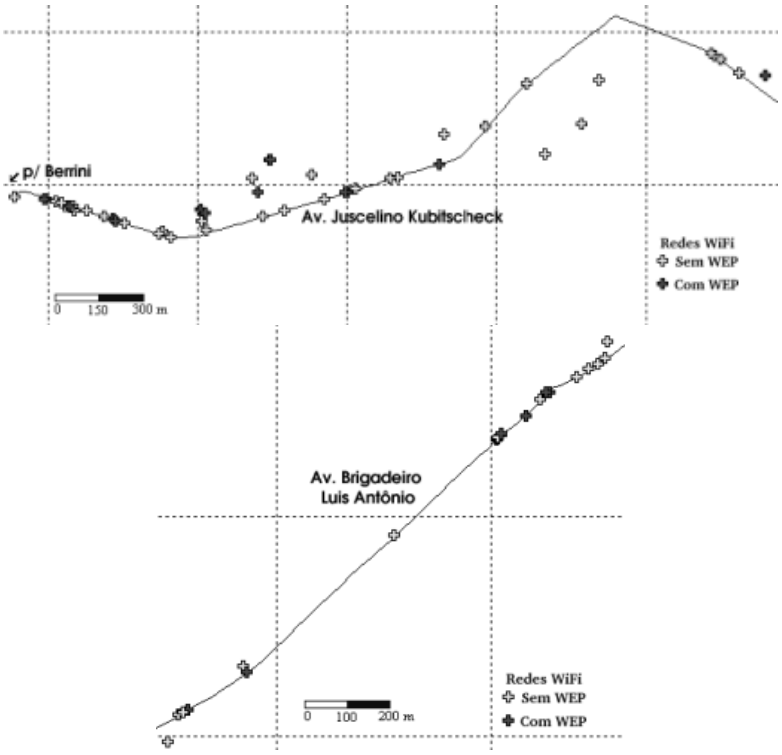


Figura 3. Distribuição das redes na região formada pelo eixo da Av. Juscelino Kubitschek (página anterior) e Av. Brigadeiro Luiz Antonio, e imediações. As marcas claras representam a detecção de redes com ausência de criptografia. Nesta região concentram-se 15.51% de redes sem criptografia, considerando-se o total de redes da pesquisa. Considerando-se apenas as redes encontradas nesta região, as redes sem criptografia somam 69.0% do total desta área.

7. CONCLUSÕES

Este trabalho apresenta evidências claras, comprovando a existencia de um problema sério nas redes sem fio das regiões estudadas. A pesquisa mostra claramente que uma parcela considerável destas redes está, no mínimo, sujeita à quebra de confidencialidade das informações trafegadas, haja vista a ausência de qualquer tipo de criptografia. Além disso, é possível inferir que estas redes também estão sujeitas a uso indevido ou outro tipo de comprometimento, visto que a quebra de confidencialidade pode evoluir para outros tipos de ataques de risco variado.

Considerando a cidade de São Paulo, as áreas pesquisadas representam um pequeno espaço amostral. Entretanto, em função da importância estratégica das regiões estudadas, onde justamente deveriam se concentrar as maiores preocupações com segurança de dados, observa-se uma situação grave e inversa, com possibilidades reais e imediatas de grande risco para estas redes sem fio, e suas interconexões.

Apesar de ser um estudo inicial, este trabalho deve servir como um sinal de alerta no sentido de uma adequação dos sistemas existentes, seja no sentido do aprimoramento e evolução tecnológica que eventualmente se torne disponível, seja no correto treinamento e capacitação dos administradores de redes para lidarem com este problema. Este último caso parece ser a indicação mais urgente mostrada por esta pesquisa.

Uma infinidade de ataques podem ser evitados facilmente, se algumas medidas simples forem tomadas quando da configuração de um concentrador de acesso de uma rede sem fio (https://www.acmesecurity.org/wireless), e dos outros dispositivos que com esta interagirão. Porém, qualquer opção adotada não significará que a rede está completamente segura. A configuração básica correta de uma rede sem fio é apenas a primeira camada de segurança de muitas outras, as quais podem ou não ser implantadas, de acordo com os princípios de usabilidade e confidencialidade necessários, e de acordo com a política de segurança da instituição.

Conforme mencionado, estes são os primeiros resultados de uma pesquisa mais abrangente. Neste momento encontra-se em curso uma série de medidas mais avançadas, que serão executadas de tal forma a aumentar o espaço amostral deste trabalho. Como exemplo, podemos citar que estão sendo feitas pesquisas de campo em diversos horários do dia e da noite, e em diversos dias da semana, de forma a possibilitar uma maior análise e interpretação dos nossos resultados. Além disso, medidas semelhantes estão sendo feitas em outras cidades de diferentes portes, para servir como meio de comparação. Em breve pretende-se publicar dados mais abrangentes desta pesquisa, mas todos os resultados preliminares estão apontando em direção às conclusões já discutidas neste trabalho.

8. AGRADECIMENTOS

Os autores agradecem a Lineu Pereira dos Santos Júnior pelo imprescindível auxílio no deslocamento e estudo logístico do percurso pesquisado na cidade de São Paulo.

9. REFERÊNCIAS

AirDefense White Paper (2002) "Wireless LAN Security – What Hackers Know That You Don't", Air Defense White Papers, Outubro, disponível em http://www.airdefense.net/whitepapers/hackers_request2.php4, acessado em Janeiro de 2004.

ANSI/IEEE Standard 802.11 (1999) "Wireless LAN Medium Access Control (*MAC*) and Physical Layer (PHY) Specifications", LAN/MAN Standards Committee of the IEEE Computer Society.

Arbaugh, W. A., Shankar, N., Wan, Y. C. J. (2001) "Your 802.11 Wireless Network has No Clothes", Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks, pp. 131 - 144, Dezembro.

Cansian, A. M., Duarte, L. O., Grégio, A. R. A. e Sacchetin, M. C. (2003) "Monitoramento Baseado na Captura de Pacotes em Redes Wireless 802.11", Proceedings of 2nd International Information and Telecommunication Technologies Symposium, pp. 18, Novembro.

IEEE Standard 802.11b (1999) "Higher-Speed Physical Layer Extension in the 2.4 GHz Band", LAN MAN Standards Committee of the IEEE Computer Society.

Park, J. S. and Dicoi, D. (2003) "WLAN Security: Current and Future", IEEE Internet Computing Vol. 7, No. 5, IEEE Computer Society, p. 60-65, Setembro/Outubro.

Peikari, C. and Fogie, S. (2002), "Maximum Wireless Security", Editora SAMS, Dezembro.

Wright, J. (2002) "Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection", HNS – Help Net Security, Novembro, disponível em http://www.net-security.org/dl/articles/l2-wlan-ids.pdf, acessado em Janeiro de 2004.

LEVANTAMENTO SOBRE A UTILIZAÇÃO DE TÉCNICAS DE MICROSCOPIA NA RECUPERAÇÃO DE DADOS EM DISCOS RÍGIDOS

Alexanders T. das N. Belarmino†, Átila Leite Romero‡, Gustavo Scarpellini de Mello‡, Marcelo de Azambuja Fortes¶ e Rafael Saldanha Campello‡.

Abstract

The magnetic force microscopy (MFM) is described as a recent method for imaging magnetization pattern with high resolution and minimal sample preparation. These features become MFM able to analyse magnetic media in order to determine the bit structure. Some Internet sites divulge the use of MFM an Scanning Tunneling Microscopy (STM) to recover previous deleted data on hard disks (HD).

This work has the goal to show the basic concepts of the Magnetic Force Microscopy and the use in magnetic media showing the first articles about the imaging of the overwritten data in Hard Disk in order to verify the viability of development of new tool of data recover.

1. INTRODUÇÃO

Um dos grandes desafios na informática forense persiste na recuperação de dados gravados em diversos tipos de mídias. Apesar de existirem no mercado mídias computacionais diversas, como discos ópticos (CD), *pen drivers*, disquetes, *zips*, *jazz*, cartões de memória e fitas DAT, o disco rígido continua desempenhando o papel de principal mídia de armazenamento, sendo provavelmente o tipo de mídia mais analisada.

Durante o processo de análise desse tipo de mídia, o perito precisa recuperar arquivos apagados, remontar tabelas de partições, trabalhar com técnicas de criptoanálise e resgatar fragmentos de arquivos perdidos em *clusters*, recuperando informações que foram descartadas mas que ainda encontram-se disponíveis no disco examinado. Apesar dessas tarefas por muitas vezes serem extremamente onerosas e exigirem um relativo nível de conhecimento, o fato de se ter acesso direto aos dados remete o problema à necessidade de automatização de tarefas, mineração e visualização de dados, técnicas em franco avanço e já encontradas em diversas ferramentas voltadas para tais propósitos.

Em um outro plano, menos freqüente mas não menos relevante, o perito se depara com problemas na leitura dos dados, causados por defeitos nos dispositivos eletrônicos que controlam o disco ou mesmo por falhas em partes eletromecânicas como motores, acionadores, etc. A solução para esses casos recai na substituição de peças como placas controladoras – tarefa extremamente simples -, elementos eletromecânicos, ou mesmo a troca de cabeças de leitura/gravação – tarefa que exige medidas mais cuidadosas e planejadas.

No entanto, o maior desafio e talvez a fonte potencialmente mais rica de informações no processo de análise forense é a recuperação de dados já sobrescritos. Recuperar mídias formatadas por diversas vezes, discos com defeitos físicos em seus substratos, arquivos apagados já sobrescritos, etc., representam o próximo passo na informática forense. Uma das alternativas indicadas para a

†SETEC/SR/DPF/SC
‡SETEC/SR/DPF/RS
¶ DITEC/DPF

recuperação de dados sobrescritos em discos rígidos[1] tem sido a técnica de microscopia de força magnética (MFM), podendo também ser aplicada em casos de defeitos físicos na mídia de armazenamento onde não se possuam as peças adequadas de reposição e a relação custo benefício seja satisfatória.

Este trabalho tem por objetivo apresentar e discutir a real utilização de técnicas de microscopia de varredura (SPM e STM) na recuperação de dados existentes na superfície de discos rígidos.

2. DISCOS RÍGIDOS – UMA BREVE ABORDAGEM DO PROCESSO DE GRAVAÇÃO E LEITURA DOS DADOS.

O disco rígido é uma mídia de armazenamento magnética de alta capacidade, composta de vários discos *("plates")* que giram em alta rotação (superior a 7.000 rpm, atualmente) inseridos no interior de uma caixa hermeticamente fechada. Junto a esses *discos* estão os cabeçotes de leitura/gravação bem como todo o aparato mecânico de movimentação dos cabeçotes e dos discos.

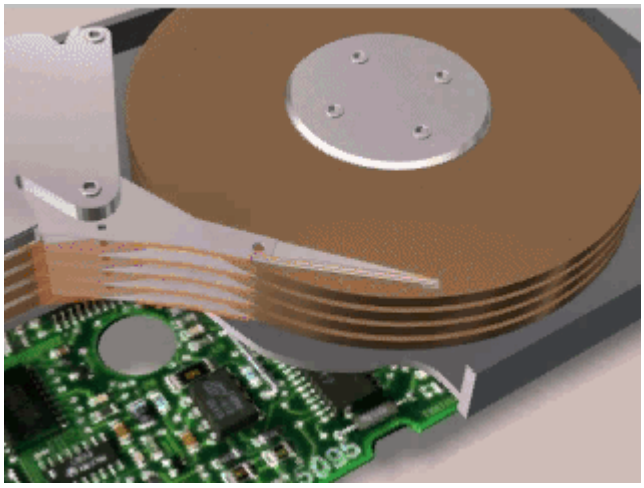


Figura 1 – Imagem dos principais componentes de um disco rígido.

Os discos magnéticos usualmente utilizados são feitos pela deposição de uma emulsão sobre uma superfície ou por filmes finos preparados por evaporação a vácuo. No método tradicional, a informação é gravada no meio em movimento através de um sinal elétrico variável no tempo, produzindo uma magnetização que varia ao longo do material. O material onde os dados são gravados deve manter a magnetização gerada durante a gravação e ao mesmo tempo permitir que a informação seja apagada (materiais que se situam entre imãs permanentes e de alta permeabilidade).[2]

Embora a tecnologia de gravação magnética tenha mais de 40 anos, o avanço da indústria exige dos pesquisadores contínuo esforço no sentido de obter mídias com grande densidade de gravação, alta fidelidade e tempo de acesso cada vez menor. As antigas cabeças de leitura eram do tipo indutivas, nas quais o campo magnético do disco induzia uma corrente na cabeça do HD. Esta tecnologia já está ultrapassada há anos, tendo sido suplantada pelas cabeças magneto-resistivas (a magneto-resistência é a propriedade pela qual a resistividade elétrica de um dado material é alterada em um campo magnético). Com essa tecnologia, a IBM anunciou um recorde de gravação de dados de 3 Gbits/in^2 em 1995 e, três anos mais tarde, noticiou a densidade de 10 Gbits/in^2, chegando a anunciar mídias com capacidade de 35 Gbits/in^2 em 1999. Novas tecnologias têm sido estudadas, incluindo cabeças de válvula giratória (baseadas no efeito magnético-resistivo gigante).

3. ESTRUTURA LÓGICA DO DISCO.

Ainda que dispositivos digitais sejam caracterizados pela manipulação de dois níveis discretos de sinais ("1s" e "0s"), o processo de leitura/gravação de dados em algum meio de armazenamento baseia-se na transição entre esses estados. Usando técnicas de codificação específicas que garantem o sincronismo e a inexistência de longas seqüências de zeros ou de "1s", os dados a serem gravados (ASCII, Unicode, etc) são traduzidos e armazenados em uma mídia magnética como transições de arranjos devidamente polarizados. Enquanto o processo de reorientação magnética – gravação – e de posterior leitura desses campos é feito pelas cabeças, toda a codificação/decodificação dos dados armazenados é realizada pela eletrônica de controle dos discos atuais, a qual usa normalmente *Run-length-limited* como método de codificação. A despeito de todo esse processo, os dados armazenados e/ou recuperados são tratados como seqüências normais de bits, tanto pelo usuário como pelo próprio computador.

4. MICROSCOPIA DE TUNELAMENTO E DE FORÇA MAGNÉTICA. CONCEITOS BÁSICOS E UTILIZAÇÃO NA ANÁLISE DE DADOS SOBRESCRITOS

As técnicas de microscopia de tunelamento (STM) e de força magnética são recentes, desenvolvidas em 1982 e 1986 respectivamente, sendo amplamente difundidas na análise de superfícies, desde o campo tecnológico até aplicações na Biologia, e propriedades magnéticas dos materiais. O impacto da microscopia de tunelamento excede o que se esperava inicialmente, sendo que o desenvolvimento da tecnologia de varreduras de *probe* associado com STM transformou-se num método eficiente para realizar medidas localizadas de diversas propriedades como: força atômica, gradientes térmicos, forças magnéticas, emissão e absorção de fótons com o uso de *probes* adequados.

A microscopia de tunelamento está baseada numa propriedade descrita na mecânica quântica: o Efeito Túnel. Em poucas palavras, este efeito prevê que uma partícula pode atravessar regiões que são proibidas classicamente devido à propriedade ondulatória da partícula, ou seja, a partícula mesmo não tendo energia suficiente para escapar (de acordo com a mecânica clássica) aparece do outro lado da barreira. A probabilidade de tunelamento de determinada partícula pode ser calculada usando a equação de Schrödinger.[3] Dessa forma, quando dois condutores são colocados a uma distância suficientemente próxima para permitir o tunelamento eletrônico, de modo que haja sobreposição das suas funções de onda, existe uma probabilidade finita de que os elétrons atravessem a barreira potencial quando um *bias* é aplicado entre as duas superfícies. O resultado é uma corrente exponencialmente relacionada com a distância entre as superfícies, sendo tal corrente dependente do material das duas superfícies.

Assim, na microscopia de tunelamento, uma ponteira condutora é mantida suficientemente próxima da superfície de modo a permitir o efeito de tunelamento, existindo dois modos básicos de análise: mantendo-se a corrente constante (variando a "altura" da ponteira) ou tendo a altura da ponteira constante (obtendo-se um sinal de corrente variável). Os sinais são recebidos e interpretados, montando-se a imagem da superfície analisada.[4]

A microscopia de força magnética (MFM), por sua vez, é um tipo de microscopia de força, da qual também faz parte a microscopia de força atômica (AFM), sendo que estas forças podem ser medidas usando um simples instrumento derivado da STM. Basicamente, um microscópio de força consiste em um sensor que responde a uma determinada força e um detector que mede a resposta deste sensor. O sensor – um tipo de haste flexível com constante de elasticidade (mola) conhecida – move-se de acordo com a força atuante na sua ponteira, força esta calculada de acordo com a Lei de Hooke ($F = k.z$).[4]

A força em um dipolo magnético com momento **m** é diretamente proporcional a densidade do fluxo magnético, o que a faz depender do gradiente do campo. Em geral, a interpretação das imagens

obtidas na MFM é complexa e requer considerável esforço teórico. Além disso, as forças magnéticas dependeram da estrutura magnética da amostra e da ponteira do sensor.

Desde o seu desenvolvimento, a MFM tem crescido em uso, incluindo a análise da estabilidade de padrões de bits em mídias de alta densidade e as características de sobrescritas dos mesmos, lembrando que acabou se tornado o método padrão na determinação do tamanho de bits, sendo aceito como uma das técnicas mais precisas para a caracterização da estrutura destes, podendo ser aplicado a diversos tipos de discos.[5,6,7]

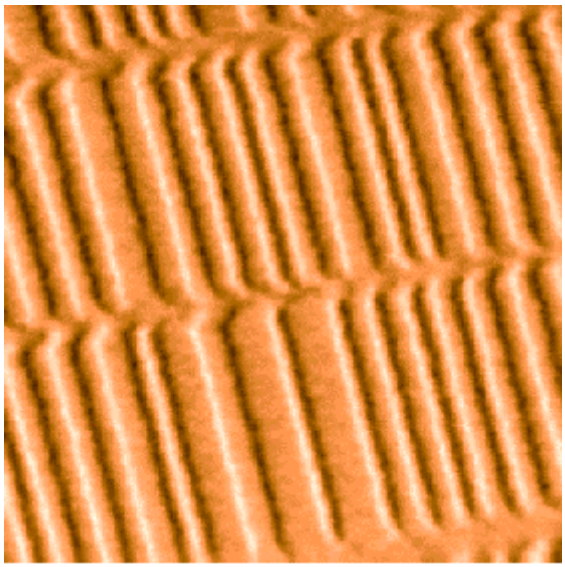


Figura 2 – Imagem de MFM de padrões de bits gravados em disco rígido.[6]

Gomez e colaboradores[8,9] estudaram o uso de microscopia de força magnética para visualizar dados sobrescritos, com o intuito de verificar a presença de bits remanescentes de gravações anteriores. Foram observadas, segundo o artigo, imagens de dados remanescentes atribuídos a pequenas variações do dispositivo eletromecânico usado para posicionamento da cabeça de gravação.

Alguns anos mais tarde, Gutmann[1] publica nos anais de um importante congresso da área de segurança um dos artigos mais contundentes sobre o assunto, reafirmando a possibilidade de recuperação de dados sobrescritos. Segundo Gutmann, quando um bit 1 é escrito sobre outro bit 1, o resultado seria equivalente ao valor 1,05, enquanto a gravação de um bit 1 sobre um zero ou de um zero sobre um bit 1 seria 0,95. Esse fato, somado ao conhecimento do padrão de bits gravados e a cabeças de leitura mais sensíveis (cita-se intensamente o uso de MFM para tal fim), seria a chave para a recuperação dos dados sobrescritos.

Em um artigo recentemente publicado em uma revista da IEEE, Simson Garfinkel e Abhi Shelat[9], pesquisadores do Instituto de Tecnologia de Massachusetts (MIT) e autores consagrados de livros na área de segurança computacional, retomam a discussão sobre a viabilidade do uso das técnicas de Gutmann nos discos rígidos atuais. A principal dúvida levantada está relacionada à alta densidade dos discos atuais, problema citado pelo próprio Gutmann em seu artigo, e à erradicação do espaço entre trilhas adjacentes deixado pelas cabeças de gravação atuais. Segundo os autores, independentemente da viabilidade teórica dos métodos descritos por Gutmann, a soma desses complicadores atuais remeteria a possibilidade de recuperação de dados sobrescritos a agências governamentais que dispusessem de grandes orçamentos aplicados a essa tecnologia (*National Security Agency*, por exemplo).

Entretanto, a crítica mais veemente ao artigo de Gutmann e à recuperação de dados sobrescritos foi recentemente feita por Daniel Feenberg[10] no site do *National Bureau of Economic Research*. Analisando detalhadamente o trabalho de Gutmann, Feenberg concentra suas críticas na incongruência entre as afirmações do artigo e as referidas bibliografias. Ele questiona o uso de MFM para a análise de grandes volumes de dados, critica a citação de alguns trabalhos meramente teóricos como se fossem trabalhos conclusivos, condena o uso de afirmações sem fundamentação bibliográfica

e, em suma, relega textualmente o artigo de Gutmann e a recuperação de dados sobrescritos à categoria de "lendas urbanas".

Do outro lado dessa discussão, profissionais dessa área baseiam-se nos rígidos padrões impostos pelos governos americano e britânico - visando à destruição de dados sigilosos - para defender que já existe tecnologia em agências desses países para a recuperação de dados sobrescritos. No governo americano, por exemplo, informações não críticas descartadas pelas suas unidades devem ser sobrescritas duas vezes, uma com valores randômicos e outra com o complemento desse valor. Mídias que armazenam dados sigilosos, por sua vez, devem ser fisicamente destruídas.

5. CONCLUSÃO

Os estudos teóricos apresentados aqui indicam que a técnica de MFM apresenta condições de ser utilizada na recuperação de dados em discos rígidos, seja em mídias danificadas fisicamente ou na leitura de dados sobrescritos que permanecem remanescentes na superfície. Essa viabilidade teórica, entretanto, está tecnologicamente muito distante das ferramentas comerciais disponíveis hoje para a análise forense.

Além disso, deve-se considerar:

- trata-se de uma técnica invasiva, existindo grande risco de danificar a mídia durante o processo de análise;
- a crescente densidade de dados na superfície dos discos é um grande limitador no uso dessas técnicas;
- os artigos sobre visualização de dados sobrescritos observaram, apenas, imagens dos dados remanescentes na superfície do disco. Outro desafio a ser vencido seria a remontagem e o tratamento dessas informações;
- mídias magnéticas, como o disco rígido, estão chegando a um limite na densidade de gravação dos dados, devendo-se acompanhar novas evoluções no desenvolvimento de técnicas de armazenamento de dados em mídias de alta capacidade para avaliar a relação custo benefício de se apostar no desenvolvimento da MFM como técnica de recuperação de dados.

Por fim, deve-se salientar a importância de investimentos maciços para o avanço nessa área de conhecimento. A exemplo da criptografia, avanços nas técnicas de recuperação de dados seriam de inegável valia no trabalho pericial.

6. REFERÊNCIAS BIBLIOGRÁFICAS.

1. Gutmann, P. **SECURE DELETION OF DATA MAGNETIC AND SOLID-STATE MEMORY.** *Artigo publicado no 6th USENIX Security Simposium Proceedings, San Jose, Ca (1996), constante no sítio www.cs.auckland.ac.nz/~pgut001/pubs/secure-del.html.*
2. Rezende, S. M. **MAGNETISMO E MATERIAIS MAGNÉTICOS NO BRASIL.** *Texto revisto em relação ao constante no Boletim no 3 da Sociedade Brasileira de Física (1998), constante no sítio www.if.ufrgs.br/pes/lam/Brasil/S_Rezende.html.*
   Atkins, P. W. **PHYSICAL CHEMISTRY.** *5th Edition. Oxford University Press. (1994).*
3. Bonnell, D. A. **SCANNING TUNNELING MICROSCOPY AND SPECTROSCOPY**. Theory, Techniques and Applications. *1st Edition (1993).*
4. Middleton, B. K. e col. **A STUDY OF RECORDED BIT PATTERN USING TEM AND MFM.** *Journal of Magnetism and Magnetic Materials, 193, 470-473 (1999).*
5. **SPM IN DATA STORAGE.** *Texto constante no sítio www.spmtips.com/bibliography/data_storage/.*
6. Rugar, D. e col. **MAGNETIC FORCE MICROSCOPY: GENERAL PRINCIPLES AND APPLICATION TO LONGITUDINAL RECORDING MEDIA**. J. Appl. Phys. 68, 1169 – 1182 (1990).
7. Gomez e col. **MAGNETIC FORCE SCANNING TUNNELING MICROSCOPE IMAGING OF**

OVERWRITTEN DATA. *IEEE Trans. Magn. 28, 3141 – 3143 (1992).*

8. Gomez e col. **MICROSCOPIC INVESTIGATIONS OF OVERWRITTEN DATA**. *J. Appl. Phys. 73, 6001 – 6003 (1993).*

9. Garfinkel, S. e col. **REMEMBRANCE OF DATA PASSED:** A STUDY OF DISK SANITIZATION PRACTICES. *IEEE Security & Privacy Jan/Febr (2003).*

10. Feenberg, D. **CAN INTELLIGENCE AGENCIES READ OVERWRITTEN DATA?** *Texto constante no sítio http://www.nber.org/sys-admin/overwritten-data-gutmann.html, (2004).*

VAZAMENTO DE INFORMAÇÕES SIGILOSAS POR E-MAIL: ESTUDO DE CASO

Murilo Tito Pereira

Perito Criminal Federal
Departamento de Polícia Federal
murilo.mtp@dpf.gov.br

Resumo

Neste trabalho relatamos uma operação policial referente ao vazamento de informações sigilosas por e-mail, supostamente de dentro de uma Instituição Federal, para uma empresa sob fiscalização de referida Instituição, descrevendo as investigações do ponto de vista pericial.

1. INTRODUÇÃO

O vazamento de informações sigilosas sempre foi um problema no mundo competitivo em que vivemos. A chegada de novas tecnologias nas empresas permite aos funcionários uma comunicação mais eficiente, contudo, essa facilidade de comunicação pode ser utilizada para repassar informações rapidamente a pessoas indevidas.

Neste trabalho descrevemos uma investigação policial referente ao vazamento de informações sigilosas por e-mail, supostamente de dentro de uma Instituição Federal, para uma empresa sob fiscalização de referida Instituição.

Apresentamos como se deram as buscas e apreensões, as informações relevantes recuperadas, o rastreamento da origem do e-mail, a estratégia da defesa, a metodologia para análise de mídias com suspeita de invasão de *hacker* e a conclusão a que chegamos.

2. PRIMEIRA APREENSÃO E RASTREAMENTO DA ORIGEM DO E-MAIL

De modo a proteger a identidade das partes envolvidas, chamaremos o Servidor Público Federal envolvido no caso simplesmente de Servidor e o Presidente da empresa sob fiscalização de Empresário.

Este trabalho começou com a apreensão de um computador que estava sendo enviado pelo empresário através dos Correios. Neste computador, entre outras informações, foram recuperados e-mails, armazenados em vários arquivos .PST do Microsoft Outlook, que continham *backup´s* de mensagens antigas. Foram encontradas quatro mensagens entre o empresário e o e-mail não identificado, que chamaremos aqui de remetente@ig.com.br.

Os conteúdos destas mensagens mostravam que o responsável pelo endereço de e-mail remetente@ig.com.br era conhecedor de informações relativas a Instituição Federal e estava repassando-as para Empresário. Dos quatro e-mails, três tinham sido enviados por remetente@ig.com.br, contudo somente um deles registrava o endereço IP de origem, no campo "X-Originating-IP: [200.226.133.250]200.XXX.97.14". O primeiro IP deste campo pertence ao IG (*Webmail* que enviou o e-mail) e o segundo pertence ao provedor utilizado pelo usuário para se conectar à Internet, sendo este o IP do usuário. As demais mensagens possuíam cabeçalho vazio,

talvez por terem sido importadas de outro programa, já que estavam armazenadas em pastas diferentes (Inbox e Caixa de Entrada).

Apesar de já termos um IP de origem, preferiu-se solicitar ao provedor IG os endereços IP´s, data e hora dos acessos à referida caixa postal. Os acessos eram realizados através do *Webmail* e os IP´s utilizados pertenciam a um mesmo provedor, verificando-se uma grande repetição dos mesmos IP´s, caracterizando o uso de IP fixo. Os *log´s* do IG revelaram uma surpresa: o IP utilizado para cadastrar a conta era do *proxy* da Instituição Federal! Ou seja, o endereço de e-mail foi criado por um usuário da *intranet* de referida Instituição. Os dados cadastrais de nome e CPF estavam consistentes, isto é, existiam e se correspondiam, mas provavelmente falsos. O endereço era o da Listel, que aparece na segunda página da referida lista telefônica.

O próximo passo foi inquirir o provedor de conexão sobre o usuário responsável pelos IP´s encontrados. Verificou-se que em determinado período o IP utilizado era o de um *proxy* rodando NAT[1], o que impossibilitava a identificação do usuário final. Durante outro determinado período, o IP utilizado estava associado a um único usuário, com conexão via *cable modem*. Constatou-se, que o contrato do referido usuário estava em nome da esposa de um Servidor Público Federal.

3. SEGUNDA APREENSÃO: ANÁLISE DOS COMPUTADORES DO SERVIDOR

Após aproximadamente três meses, foi realizada a busca e apreensão na residência e na sala de trabalho do Servidor e decretada sua prisão. Em sua residência foram apreendidos, entre outros materiais, cinco computadores (sendo dois notebooks) e mais um em sua sala de trabalho.

Devido ao uso de *Webmail* para enviar os e-mails, somente foram encontrados dois fragmentos de arquivo relacionados ao caso em questão, em dois computadores diferentes. Estes fragmentos não possuíam cabeçalho de arquivo que pudessem indicar o nome ou data de criação/alteração.

Um deles era um texto que tratava do mesmo assunto dos outros e-mails encontrados, sem o cabeçalho típico de e-mail (remetente/destinatário/assunto), que foi escrito no Microsoft Word. Foi realizada uma recuperação de arquivos apagados, porém não foi recuperado o cabeçalho deste arquivo. Contudo, no campo de propriedades do Word, está registrada a data de criação igual a 30/04/2001 e o autor igual ao nome do Servidor.

O outro fragmento, apesar de não apresentar conversas, era bem interessante, e está transcrito a seguir, sendo o número de linha colocado por nós:

Linha	Conteúdo	Linha	Conteúdo
1	*last_InMail*	*10*	*InMail1*
2	*remetente@ig.com.br*	*11*	*remetente@ig.com.br.InMail2*
3	*ig.com.br/*	*12*	*ig.com.br/*
4	*0*	*13*	*0*
5	*179800576*	*14*	*3834229248*
6	*29461069*	*15*	*29452337*
7	*2683290624*	*16*	*2683290624*
8	*29443606*	*17*	*29443606*
9	*	*18*	*

Este fragmento era originalmente um arquivo de *cookie*, que atingiu sua data de expiração, sendo excluído automaticamente pelo Internet Explorer, restando somente os dados do arquivo, e perdendo-se o cabeçalho. O *cookie* acima demonstra acesso ao e-mail remetente@ig.com.br, possuindo duas partes, sendo a primeira referente às linhas 1 a 9 e a segunda às linhas 10 a 18. Os números que aparecem nas linhas 7/8 e 16/17 representam a data de criação do *cookie* e os que

[1] NAT (Network Address Translation) é um padrão da Internet que permite que uma rede de IP´s não válidos utilize um único IP válido para acessar a Internet, ou seja, todos os usuários vão acessar a Internet com o mesmo IP.

aparecem nas linhas 5/6 e 14/15, a data de expiração. Realizando a interpretação destes dados, temos que as datas de criação e expiração da primeira parte do *cookie* são 25/09/01 e 21/12/01, respectivamente, e as datas de criação e expiração da segunda parte do *cookie* são 25/09/01 e 08/11/01, respectivamente.

É interessante notar que o disco rígido com o fragmento de Word teve o SO re-instalado, com possível formatação, após a data de criação do arquivo referente a este fragmento. O Laudo foi entregue apontando estes dois fragmentos como a confirmação do uso destes dois computadores para acesso ao endereço de e-mail remetente@ig.com.br.

4. TESE DA DEFESA: INVASÃO DE HACKER

Após algum tempo, fui chamado, na Justiça Federal, para prestar esclarecimentos sobre os Laudos. Neste momento, a tese da defesa foi apresentada: "seria possível um *hacker* ter invadido os computadores do acusado e enviado os e-mails a partir deles, de forma a incriminá-lo?"

A tese da defesa sugere uma conspiração contra o Servidor, pois ela não tenta negar as provas, e sim, imputá-las a outra pessoa, que, no caso, teria feito as ações com a intenção deliberada de incriminá-lo.

Na Justiça Federal foram 17 perguntas efetuadas pelo Juiz, nenhuma pelo Ministério Público e 60 pela Defesa. Ou seja, apesar do questionamento ser um só, foram feitas várias perguntas do tipo "em tese, é possível acontecer tal coisa?", o que no campo da informática é sempre possível, apesar de improvável. Exemplos de perguntas: "é possível inserir/editar um fragmento em um disco rígido?", "é possível os funcionários dos provedores alterarem os arquivos de *logs*?", "é possível um *hacker* invadir um computador e enviar um e-mail a partir dele?", "é possível haver um seqüestro de IP", "é possível editar um arquivo .PST (Microsoft Outlook) de forma a inserir mensagens recebidas e enviadas?".

Em nenhum dos dois laudos entregues (computador do Empresário e computadores do Servidor) foi realizado procedimento para verificação de possível invasão de *hacker*, pelo fato de não ter sido solicitado e de não se tratar de um exame rotineiro. Sabemos que este tipo de exame é bastante complexo, mas nos colocamos a disposição da Justiça Federal para realizá-los.

Somente após nove meses chegou a nova solicitação de Laudo sobre a possível invasão de *hacker*. Havia quesitos do Juiz, do Ministério Público e da Defesa. Entre quesitos bem elaborados e simples como "Há programas de acesso remoto no computador ou programa espião?" ou "Realizar busca e verificação da possível existência de *trojan horses* e *backdoors*", também havia quesitos exóticos como "Relacionar todos os Programas instalados no computador, com suas versões e possíveis correções (*service packs*)" ou "Informar os *log´s* de todos os registros de inicialização".

5. METODOLOGIA PARA ANÁLISE DE MÍDIAS SUSPEITAS DE INVASÃO POR HACKER

Antes de explicar a metodologia utilizada nos exames, mostraremos a configuração de rede dos computadores do Servidor acusado. Ele possuía uma rede local em sua residência, com conexão a Internet via *cable modem*. Um dos computadores possuía duas placas de rede e funcionava como gateway, utilizando um endereço IP válido do provedor de conexão, atribuído por DHCP, e outro não válido. Os demais computadores possuíam endereços IPs não válidos. O *notebook* que possuía o *cookie* só tinha configurado, no momento da análise, acesso à Internet por *dial-up*. Os Sistemas Operacionais eram Windows 98 e XP. Vale observar que os computadores foram devolvidos, ficando apreendidos só os discos rígidos. Todas essas informações da rede foram extraídas diretamente da configuração do Windows.

Na busca por invasão por *hacker* dois fatos específicos deste caso mudaram bastante o cenário: em primeiro lugar, como dito anteriormente, a tese da defesa sugere uma conspiração. No caso de um acesso por *dial-up,* o usuário estará tão vulnerável a ataques impessoais quanto no acesso dedicado, porém o fato de estar utilizando IP dinâmico, em um dos computadores, diminui consideravelmente a chance de um ataque como forma de conspiração. O atacante não sabe o momento que o alvo (Servidor) está conectado, nem qual o IP que ele está utilizando.

Em segundo lugar, a existência do arquivo de *cookie* indica que o acesso ao e-mail remetente@ig.com.br foi feito via *Webmail*, quer dizer, via navegador, abrindo a página do provedor de e-mail www.ig.com.br, entrando com usuário e senha, e executando comandos para o envio do e-mail. Os *logs* do provedor confirmam que o acesso ao referido e-mail era via *Webmail*.

Quando se imagina que um *hacker* invade o computador de um usuário com o intuito de enviar um e-mail a partir deste para que fique registrada, no provedor, a origem como sendo o usuário, não se imagina que ele usará as ferramentas próprias do usuário para envio de e-mail, que são os programas de correio eletrônico ou, neste caso, o acesso via *Webmail*. O comum, para um *hacker*, é que fossem utilizadas ferramentas de "linha de comando" e não utilizando interfaces gráficas com menus, mouse, etc. Isto acontece porque a invasão normalmente fornece um acesso precário ao computador do usuário, não em termos de privilégios de execução, mas em termos de interface. Ou seja, explorar uma vulnerabilidade que permita controle total da máquina alvo, não significa exatamente poder fazer qualquer coisa, pois são necessários softwares apropriados para realizar ações específicas. É importante explicar isto no Laudo, pois as notícias sobre vulnerabilidades de programas falam de controle total e a defesa pode usar isto, até por falta de conhecimento, a seu favor.

Esta interface de linha de comando não é visualizada ou percebida na máquina invadida e é mais do que suficiente para o envio de um e-mail a partir da máquina invadida. Vale lembrar que para o envio de e-mail não é necessária autenticação (senha), somente para o recebimento. Logo, seria-se de esperar que o envio do e-mail se desse via linha de comando.

Contudo, conforme dito, a existência do *cookie* indica que o acesso ao e-mail remetente@ig.com.br foi feito via *Webmail*. Esta opção não é natural para um *hacker* por dois motivos: a) necessidade de instalar uma ferramenta que permitisse o controle remoto do desktop (ambiente de trabalho) do usuário, ou seja, uma ferramenta que permitisse a visualização da tela do usuário, controle do mouse, teclado, etc; b) o uso desta ferramenta chamaria a atenção do usuário, pois o mesmo veria seu computador "trabalhando sozinho", isto é, abrindo programas, digitando conteúdo de e-mails e os enviando.

Ferramentas desta natureza existem para atividades lícitas, por exemplo o *PCAnyWhere*, em que numa rede corporativa o técnico de suporte pode acessar remotamente o computador de um usuário com problema e resolvê-lo sem precisar se deslocar. Também existem as ilícitas, tipo *trojan horse*, por exemplo *SubSeven*, que permitem um controle remoto da máquina invadida. A diferença entre as duas, além das funcionalidades, é que a lícita é instalada pelo usuário ou administrador, não estando oculta do mesmo, enquanto a ilícita é instalada sem conhecimento do usuário/administrador, ficando oculta.

Pelo exposto, concluiu-se que deveria haver instalado um software de controle remoto, provavelmente ilícito (*trojan horse*).

O procedimento utilizado para a detecção deste tipo de software e a determinação da invasão por *hackers* foi o seguinte:

I. Busca por trojan horses: foram utilizados dois programas para a busca por trojan horses – PestPatrol [7] e TrojanHunter [8]. O programa PestPatrol busca por mais de 20000 tipos de "pestes", que incluem Trojan, Backdoor, Worm, Key Logger, Password Capture, Hijacker, Hostile ActiveX, Hostile Java, entre outros, enquanto o programa TrojanHunter procura especificamente por trojan horses, possuindo, em maio de 2004, 3930 definições de trojans. Além disto, para verificar a possibilidade de um trojan ter sido instalado e posteriormente apagado, foi realizada a recuperação de todos os arquivos apagados, e estes foram incluídos nos arquivos a serem procurados por trojan horses.
II. Execução de software tipo scanner de portas: um trojan horse ou programa espião instalado em um computador terá, necessariamente, que deixar uma porta aberta (backdoor) para que seja realizada uma conexão remota. Um software tipo scanner de portas faz uma varredura

de todas as portas abertas no computador alvo, verificando qual serviço está rodando em cada porta aberta. O software utilizado foi o Nessus [6] que faz a varredura por portas abertas, identifica e testa, sempre que possível, o serviço associado a cada porta e mostra um relatório identificando as possíveis vulnerabilidades do serviço.

O fato de a apreensão dos computadores questionados ter ocorrido a quase um ano facilita o trabalho de detecção de possível invasão, pois por mais moderna que tenha sido a técnica utilizada, no momento dos exames ela já teria se tornada conhecida e, conseqüentemente, detectável pelos softwares citados.

Os resultados destas análises foram:

I. Não foi detectado nenhum *trojan horse* ou programa de controle remoto instalado.
II. O *scanner* de portas encontrou vários serviços sendo executados. Os mais comuns, o próprio programa já verificava e testava o serviço, e os outros mais específicos ele só reconhecia a porta aberta. Neste segundo caso, era necessário que verificássemos o programa associado à referida porta, observando se tratava de um programa lícito ou não. Constatou-se que não havia nenhum serviço ilícito sendo executado.
III. Foram encontradas várias vulnerabilidades, principalmente no Windows XP e em programas de comunicação, como, por exemplo, o Kazaa. Contudo, não havia qualquer indício de que elas tivessem sido exploradas.

Chegou-se a conclusão, então, que não há instalado programa que permita o controle remoto das máquinas apreendidas.

6. OUTRAS EVIDÊNCIAS

Além das apresentadas, outras evidências corroboram o envolvimento do Servidor com o empresário:

I. O apelido e telefone do empresário armazenados na agenda de um dos celulares do Servidor. Inapropriadamente, os agentes que participaram da busca e apreensão manusearam o celular, podendo resultar na não aceitação desta prova.
II. O apelido e o telefone do empresário (diferentes dos anteriores) armazenados na agenda eletrônica do Servidor. A agenda foi enviada para a perícia em saco plástico lacrado, não havendo motivos para desqualificar a prova.
III. O Servidor possuía, em documentos oficiais, os dados da pessoa dona do nome e CPF utilizados para abrir a conta de e-mail remetente@ig.com.br.

7. CONCLUSÃO

Neste trabalho, descrevemos uma estratégia de análise de mídias suspeitas de invasão por hacker aplicável, principalmente, nos casos onde é necessária a instalação de programas de controle remoto.

No caso em estudo, as provas apresentadas (mensagem na máquina do Empresário, rastreamento da origem do e-mail, fragmentos de e-mails na máquina do Servidor, verificação de que não houve invasão de *hacker* e as outras evidências coletadas) levam a crer que o Servidor realmente era o responsável pela referida conta de e-mail.

Acreditamos que os crimes envolvendo Internet serão freqüentemente contestados pela defesa com a tese de invasão de *hackers*, e a perícia deve se preparar para realizar tais exames, bem como buscar outras evidências que comprovem ou não o ato em questão.

8. BIBLIOGRAFIA

[1] Comer, D. Internetworking with TCP/IP Vol.1, Prentice Hall, 2000.
[2] Costa, R. G. P. e Ribeiro, S. F. Desvendando e Dominando o Registro do Windows, Ciência Moderna, 2004.
[3] Mandia, K. e Prosise, C. Hackers: Resposta e Contra-ataque: investigando crimes por computador, Campus, 2001.
[4] O´dea, M. Hack Notes: Segurança no Windows, Campus, 2004.
[5] Tanenbaum, A. S. Redes de Computadores, Campus, 2003.
[6] www.nessus.org.
[7] www.pestpatrol.com.
[8] www.trojanhunter.com.

MÁQUINA CAÇA-NÍQUEL: UMA ABORDAGEM SOB A LUZ DA IT 001-2004-GAB/DITEC/DPF

José Helano Matos Nogueira
Perito Criminal Federal
Setor Técnico Científico
Departamento de Polícia Federal
SETEC/SR/DPF/CE

Marcelo de Azambuja Fortes
Perito Criminal Federal
Diretoria Técnico-Científica
Departamento de Polícia Federal
DITEC/DPF

E-mail: {helano.jhmn, fortes.maf}@dpf.gov.br

ABSTRACT

The criminal police expert is in charge carrying through the most diverse types of examinations, however, is necessary that the connoisseurs are prepared for the new practical types of delictual, its used disguises, ways and instruments. In the last years, it has been common the apprehension of machines of the type slot machines ("caça-níqueis") in the most diverse places of the Brazilian territory. With these electronic-computational equipment it is possible to evidence diverse practical delictual as game of chance, contraband, embezzlement, elimination and fiscal tax evasion.

1. INTRODUÇÃO

A perícia criminal está encarregada de realizar os mais diversos tipos de exames, todavia, é preciso que os peritos estejam preparados para os novos tipos de práticas delituosas, seus disfarces, meios e instrumentos utilizados. Nos últimos anos, tem sido comum a apreensão de máquinas do tipo caça-níqueis nos mais diversos locais do território brasileiro. Com estes equipamentos eletrônico-computacionais é possível constatar diversas práticas delituosas como jogo de azar, contrabando, descaminho, elisão e sonegação fiscal, dentre outras correlatas e disfarçadas em seu ambiente de funcionamento.

Este trabalho visa esclarecer a comunidade pericial com o embasamento legal em vigor e como realizar o exame e a elaboração do Laudo em Equipamento Eletrônico, mais especificamente Máquina Caça-Níquel. Para isso, será feita uma abordagem casuística com estudo de casos do ponto de vista da criminalística da forma mais pragmática possível. A partir de então se almeja que de posse destes conhecimentos peritos, delegados, promotores, procuradores espalhados em todas as regiões possam elaborar seus futuros trabalhos com mais segurança e eficácia que casos desta sorte exigem. Entretanto, não se procura com este trabalho exaurir o tema, mas sim, traçar metodologias e abrir o leque de discussão sobre o assunto.

2. CONCEITUAÇÃO NECESSÁRIA

Para a realização dos exames e procedimentos que visem adequação ao sistema legal vigente os seguintes conceitos são de grande relevância:

I – máquina caça-níquel: máquina de jogo que funciona por meio da introdução de valores monetários, geralmente em moedas, e que paga um prêmio, igualmente em valores monetários, àquele que acertar as combinações previstas;

II – jogo de azar: jogo em que o ganho ou a perda depende exclusiva ou principalmente da sorte;

III – sorte: maneira de decidir alguma coisa pelo acaso. Fato resultante de causa independentemente da vontade;

IV - Principais componentes, partes e peças das máquinas do tipo "caça-níqueis" são: a placa-mãe ou placa de CPU/UCP (unidade central de processamento), o microprocessador, a placa de circuito impresso, o circuito integrado (chip), o analisador de valores monetários (fichas, moedas, cédulas) e o rotor (*hopper*).

3. HISTÓRICO E EMBASAMENTO LEGAL PERTINENTE

A base normativa utilizada para a realização dos referidos exames periciais está fundamentada, nos seguintes dispositivos legais:

I – Decreto-Lei 2.848, de 7 de dezembro de 1940, com redação dada pela Lei 4.729, de 17 de julho de 1965 – Código Penal;

II – Decreto-Lei 3.689, de 3 de outubro de 1941 – Código Processual Penal;

III – Decreto-Lei 3.688, de 3 de dezembro de 1941 – Lei das Contravenções Penais e;

IV – Instrução Normativa SRF 309, de 18 de março de 2003, publicada no DOU de 21 de março de 2003.

V – Instrução Técnica Nº. 001-GAB/DITEC/DPF, de 04/05/2004.

4. MATERIAL QUESTIONADO

Após o esclarecimento legal que existe por trás de jogos em máquinas deste tipo, o primeiro passo na elaboração do Laudo em Equipamento Eletrônico (Máquina Eletrônica Programável ou Máquina Caça-níquel) começa pela descrição do material questionado submetido a exame. Com a globalização do mercado e a facilidade de compra e venda através do comércio internacional, as novas marcas e modelos de máquinas caça-níqueis estão em constante modificação. Logo se vê que a perícia como um todo necessita de uma atualização sistemática que possa acompanhar toda essa dinâmica ora imposta pelos recursos tecnológicos. Nada desesperador, a estrutura básica destes equipamentos continua a mesma. O importante nesta seção é identificar e descrever de forma clara e segura os componentes relevantes que fazem parte do instrumental examinado de forma a manter a unicidade do material em questão e deste modo evitar que haja troca de material, extravio ou a sua perda.

A identificação de forma unívoca é a chave para conclusão desta primeira etapa de elaboração do laudo. Traçando um paralelo com outros tipos de laudos, a descrição do material questionado, no caso, máquina caça-níquel, nada mais é do que realizar um exame mercelógico, com a vantagem de não precisar quantificar em valores financeiros as suas partes e peças.

Logo, o material apreendido e apresentado como questionado, constituído essencialmente de máquina do tipo caça-níquel, deve ser detalhadamente especificado, de modo a não deixar dúvida na sua caracterização e posterior identificação. Sempre que possível, deve-se destacar:

I – a quantidade de máquinas apresentadas a exames;

II – o modelo ou nome de fantasia;

III - o número de série;

IV – a origem;

V – as características externas; e

VI – as condições de funcionamento e o estado da máquina quando dos exames, com indicação das avarias e danos observados.

Algumas etapas podem ser realizadas conforme abaixo:

Havendo mais de um modelo de MEP, os exames deverão ser realizados em, pelo menos, cada um deles.

A nomenclatura do modelo impresso na face externa da MEP deve ser confirmada com o jogo apresentado na tela, após a máquina ser colocada em funcionamento.

Em caso de divergência, prevalece o tipo de jogo apresentado na tela da MEP.

Quando se constatar mais de um número de série, deve ser informado o mais completo, observável nas inscrições encontradas nas partes, peças e etiquetas fixadas nas máquinas.

A origem ou procedência a ser indicada é a constatável na etiqueta ou inscrição afixada na MEP.

As características externas correspondem à cor, ao tipo do material utilizado, aos detalhes visuais observáveis, às dimensões de altura, largura e profundidade do gabinete no qual a MEP está montada.

Deve ser informado se a máquina está construída sobre algum tipo de pedestal.

Devem ser descritas as faces: anterior (frontal), posterior (traseira) e laterais, se possível.

Sempre que possível, cada modelo de MEP examinada deve ser fotografado.

Visando facilitar o modo de descrição do equipamento examinado pode ser criada uma tabela contendo os seguintes campos (colunas) informativos:

I – item - quando há um grande volume de equipamentos a ser periciado este campo deve ser introduzido pelos Peritos signatários para facilitar a organização e controle;

II – número de série;

III – modelo;

IV – origem ou procedência;

V – condições de uso - informar se equipamento está em condições adequadas de funcionamento na época dos exames;

VI – observações - corresponde ao estado em que a máquina se encontrava à época dos exames, indicando as avarias e danos apresentados nos equipamentos;

VII – valor total das moedas - informar o valor total, em moedas, no padrão monetário brasileiro ou estrangeiro, conforme o caso, encontrado no interior dos equipamentos quando dos exames;

VIII – valor total das cédulas - informar o valor total, em cédulas, no padrão monetário brasileiro ou estrangeiro, conforme o caso, encontrado no interior dos equipamentos quando dos exames.

5. REALIZAÇÃO DOS EXAMES PERICIAIS

Neste tópico são realizados os procedimentos periciais de verificação e teste das máquinas. Somente após os exames realizados é que o perito pode chegar a alguma conclusão plausível. De uma forma sucinta, mas eficaz e didática, esta seção pode ser subdividida em descrição, mecanismo de programação, funcionamento do jogo e estatísticas de jogadas.

Constar no laudo que os exames e análises técnico-científicas foram realizados com base neste Parecer Técnico.

5.1. Exames Gerais

Antes de ligar as máquinas questionadas verificar se há compatibilidade da tensão elétrica das mesmas com a rede elétrica pública.

Procurar danos e avarias materiais aparentes nos equipamentos.

Descrever os principais componentes, partes e peças internas das máquinas (vide conceituação anterior). Identificar a origem dos principais componentes, se possível.

Após a abertura das máquinas verificar a forma de introdução dos valores para realizar jogadas, se são utilizadas moedas ou cédulas. Todos os valores monetários em moeda nacional ou estrangeira encontrados no interior das máquinas devem ser contados e acondicionados para que seja feito um depósito judicial pela autoridade solicitante. Tal contagem de valores monetários deve ser feita preferencialmente por Escrivães.

5.2. Funcionamento dos Jogos

Explicar sucintamente o funcionamento dos jogos. Para isto retirar amostra de um exemplar de cada modelo, consultando, quando possível, manuais do fabricante, telas de apresentação ou jogando.

Algumas máquinas podem conter mais de um jogo em funcionamento, portanto, enquadrando-se em vários grupos, por exemplo, a máquina modelo PICK A GAME.

Visando a finalidade organizacional do laudo e a sua apresentação, as MEPs do tipo caça-níquel podem ser divididas em grupos, tais como apresentados a seguir:

Grupo I – (Meps com painel luminoso para sorteio aleatório de símbolos ou figuras)

Em seguida são apresentados alguns modelos já periciados em laudos anteriores a este parecer e que podem ser enquadrados neste grupo:

CAMPEONATO BRASILEIRO	CAR BINGO	CAVEIRA
CAVEIRA II	CAVEIRINHA	CAVEIRINHA PLUS
COPA	COPA 2002	COPA 2002 PLUS
COPA 98	COPA 98 II	COPA DO BRASIL
COPA MASTER	FUTEBOL 2000	HELL FIRE
J P MÁRIO	MÁRIO	MINI BINGO GOL PLUS
MINI MÁRIO	MINI MARIO FUTEBOL 2000	OLIMPÍADA 2000
SOCCER 2000		

Grupo II – (MEPs com cilindros ou suas simulações em vídeo)

Em seguida são apresentados alguns modelos já periciados em laudos anteriores a este parecer e que podem ser enquadrados neste grupo:

21ST CENTURY BINGO	21ST CENTURY SLOT	BAR 7
BINGO MANIA	BINGO SLOT	BINGO STAR
BINGO SWAMP	BINGO TOTAL	CHERRY GAME
CHERRY MASTER	DIGGER'S GOLD	GOLD EAGLES
GREATEST HITS	JEWELS CHEST	KENO 2000
KENO MANIA	KING DIAMONDS	LOTO MANIA
LUCKY WORLD	MAGIC CASHIER	MAGIC BINGO
MEGA SAURUS	MINI BINGO MANIA	MINI BINGO GOL PLUS
MONEY MAKER	NEPTUNE'S PEARLS	ORIENTAL LEGEND
PICK A GAME	REELS ROYCE	SAMBA
SPICY SPINS	SWAMP LAND	TURF CLUB
TWIN SPARKS	TYCOON	

Grupo III – (MEPs baseadas em cartas de baralho ou suas simulações)
Alguns modelos enquadrados nesta categoria:

DEUCE'SWILD	JOKER'S WILD	MINI BALL POKER
NOVO POKER II	VIDEO POKER	WINNING JOKER

Grupo IV – (MEPs baseadas em cartelas de bingo ou suas simulações)
Alguns modelos enquadrados nesta categoria:

BINGO	BINGO 5	DIAMOND DOG
KENO	PICK A GAME	REAL BINGO
SUPER BINGO	TOP MASTER	VIDEO BINGO

Grupo V – (MEPs baseadas em Roletas)

Modelo enquadrado nesta categoria:
ROLETA ELETRÔNICA

6. CONCLUSÃO

O intuito primordial deste trabalho foi passar a experiência adquirida em vários casos elaborados sobre o assunto e apresentar de forma clara e objetiva como elaborar o Laudo em Equipamento Eletrônico (Máquina Eletrônica Programável ou Máquina Caça-níquel). Para isso, o laudo foi dividido em seções: considerações gerais, histórico e embasamento legal, material questionado, exame e respostas aos quesitos, tornando-se, portanto, o mais realista possível. Vários procedimentos foram abordados de modo prático visando facilitar e direcionar os procedimentos de atuação da criminalística segundo o enfoque pericial.

Este trabalho está longe de ser uma obra completa no tange a este tipo de laudo pericial, mas, com ele, será possível dirimir dúvidas que surgem durante a feitura do laudo. Dúvidas estas que vêm aumentando assustadoramente em algumas seções de criminalística. A partir deste trabalho espera-se que sejam abertos novos horizontes e que sejam traçados novos rumos onde os peritos possam caminhar de modo firme e seguro em direção a conclusão de seus laudos em máquinas do tipo caça-níqueis.

7. BIBLIOGRAFIA

[1] Nogueira, José Helano Matos, *Máquinas Caça-Níqueis*, Brasília: Revista Perícia Federal, Ano IV, Nº 12, páginas 11-18, março/2002.

AGENTES INTELIGENTES MÓVEIS NO COMBATE AS INVASÕES CIBERNÉTICAS

José Helano Matos Nogueira

Perito Criminal Federal
Setor Técnico Científico
Departamento de Polícia Federal
SETEC/SR/DPF/CE
helano.jhmn@dpf.gov.br

1. INTRODUÇÃO

A informação mantida em sistemas computacionais tem se tornado um recurso cada vez mais crítico para o alcance dos objetivos e metas das organizações. Para muitas pessoas, as redes de computadores representam uma nova era na comunicação humana. O anonimato na comunicação, por exemplo, via Internet, sugere que a rede de computadores é um lugar seguro e sem práticas ilícitas. Infelizmente, esse ponto de vista utópico não é realista. Existem práticas criminosas no espaço cibernético em quantidades já preocupantes. As invasões cibernéticas não possuem uma linha de frente, os campos de batalha estão em qualquer lugar do globo com sistemas em rede que permitam o acesso a grande rede mundial. As possíveis vulnerabilidades e as formas de ameaça estão se espalhando, antes restritas a especialistas e estudiosos, nos dias atuais passam a estarem disponíveis de forma gratuita na Internet. É chegada a hora de refletir e combater estes novos tipos de crimes que surgem no mundo virtual.

A tecnologia de agentes inteligentes vem mudar radicalmente o modo como o usuário utiliza o computador, permitindo que o software seja um assistente ao usuário. Esta tecnologia deverá aproximar ainda mais o usuário ao seu computador. Essa tecnologia é, atualmente, uma das áreas de pesquisas que representa um grande interesse em desenvolvimento de novas aplicações. Ela expõe ao usuário facilidades que são baseadas em conceitos da Inteligência Artificial Distribuída (IAD). Nas abordagens clássicas de Inteligência Artificial (IA), a ênfase da inteligência é baseada em um comportamento humano individual e o foco de atenção volta-se à representação do conhecimento e métodos de inferência. Já a IAD é baseada em comportamento social e sua ênfase é para cooperações, interações e para o fluxo de conhecimento entre unidades distintas. Na resolução distribuída de problemas, os agentes cooperam uns com os outros, dividindo e compartilhando conhecimentos sobre o problema e sobre o processo de obter uma solução. Nesta abordagem, os agentes são projetados especificamente para resolver problemas ou classe de problemas, coordenando ações definidas em tempo de projeto. No caso de sistemas multiagentes, o projetista não volta sua atenção para um problema específico, mas para um domínio específico. Nesta abordagem, a idéia consiste em coordenar o comportamento inteligente de um conjunto de agentes autônomos móveis, cuja existência pode ser anterior ao surgimento de um problema particular. Os agentes devem raciocinar a respeito das ações e sobre o processo de coordenação em si. As suas arquiteturas são mais flexíveis e a organização do sistema está sujeita a mudanças visando adaptar-se às variações do ambiente e/ou do problema a ser resolvido.

Portanto, este trabalho visa esclarecer a comunidade pericial e a sociedade em geral sobre o problema das invasões cibernéticas e como combatê-las usando a tecnologia de agentes inteligentes móveis que navegam sob redes de computadores.

2. AGENTES

A definição mais geral sobre agentes refere-se a agentes como: uma entidade real ou virtual que emerge num ambiente onde pode tomar decisões, que é capaz de perceber e representar parcialmente esse ambiente, que é capaz de comunicar-se com outros agentes e que possui um comportamento autônomo que é uma conseqüência de sua observação, seu conhecimento e suas interações com outros agentes. Agente é uma entidade cognitiva, ativa e autônoma, ou seja, que possui um sistema interno de tomada de decisões, que age sobre o mundo e sobre os outros agentes que o rodeiam e, por fim, que é capaz de funcionar sem necessitar de algo ou de alguém para o guiar com mecanismos próprios de percepção do exterior, vide figura 1. Uma outra definição, agora mais computacional, é a que descreve um agente como sendo um programa de software que auxilia o usuário na realização de alguma tarefa ou atividade. Embora não haja ainda um consenso sobre uma definição formal do que seja o agente de forma que englobe todo o espectro possível, algumas características esperadas foram estabelecidas.

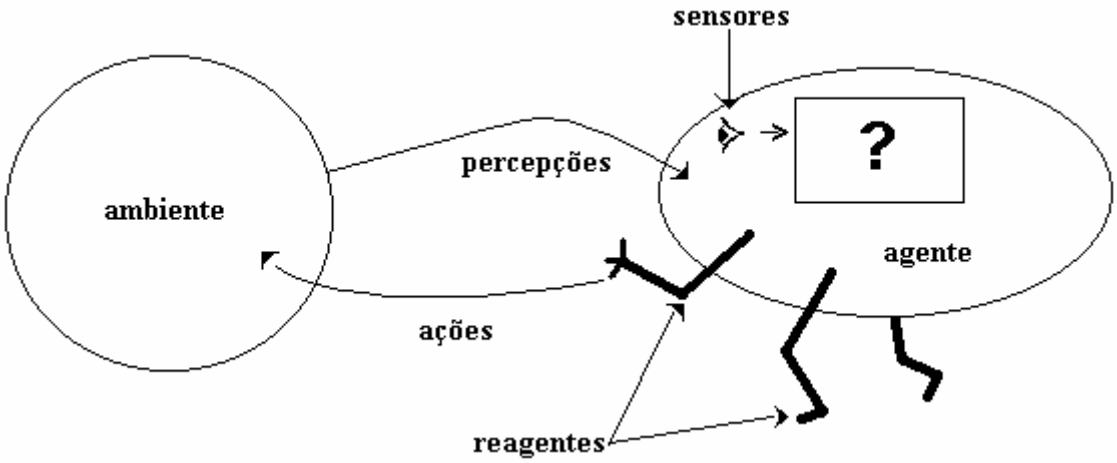


Figura 1 – Interação do agente com o ambiente

2.1. Características Esperadas dos Agentes

Alguns atributos que caracterizam os agentes no mundo cibernético são:

Mobilidade: é a habilidade de um agente mover-se em uma rede;

Solicitude: é a suposição de que os agentes não têm objetivos contraditórios e que todo agente sempre tentará fazer o que lhe é solicitado;

Racionalidade: é a hipótese de que um agente agirá de forma a alcançar seus objetivos;

Adaptabilidade: um agente deve ser capaz de ajustar-se aos hábitos, métodos de trabalho e preferências de seus usuários;

Colaboração: um agente não deve aceitar e executar instruções sem considerações, mas deve levar em conta que o usuário humano comete erros, omite informações importantes e/ou fornece informações ambíguas. Neste caso, um agente inteligente deve checar estas ocorrências fazendo perguntas ao usuário.

2.2. Aplicação Apropriada para Agentes

A seguir são identificadas algumas áreas de aplicação para uso da tecnologia de agentes:

Segurança de Redes: Esta é uma das áreas mais promissoras para empregar a tecnologia de agentes inteligentes móveis. O uso crescente de arquiteturas em redes e sistemas distribuídos elevou a complexidade dos sistemas em operação, principalmente em redes locais. As arquiteturas de agentes

empregadas são, em sua maioria, não inteligentes, entretanto sistemas inteligentes encontrariam muitas aplicações em níveis mais altos de abstração, por exemplo, aprendendo a reagir a determinados padrões no comportamento dos sistemas. Além disso, poderiam ser também empregados no gerenciamento dinâmico de grandes configurações;

Acesso e Gerenciamento Móvel: Na medida em que a computação vai se tornando cada vez mais distribuída e difusa, surge a necessidade dos usuários empregarem tecnologias móveis, tais como comunicações sem fio. Os agentes poderiam conecta os usuários a partir de qualquer lugar e ainda não sofrer as restrições de largura de banda por vezes impostas pelas telecomunicações;

Correio Eletrônico e Troca de Mensagens: Agentes vem sendo empregados nesta área já há algum tempo, priorizando mensagens e organizando automaticamente o correio eletrônico de seus usuários. Os agentes inteligentes podem facilitar todas essas funções, por exemplo por meio de regras que poderiam ser inclusive deduzidas a partir de padrões de comportamento observados em seus usuários;

Colaboração: É uma área em rápido crescimento onde os usuários trabalham juntos em documentos compartilhados na rede. Aqui é necessário não apenas uma infra-estrutura que permita o compartilhamento robusto e escalável de dados e outros recursos, mas também funções que permitam gerenciar equipes e o produto de seu trabalho. O exemplo mais conhecido de aplicações deste tipo é o Lotus Notes;

Interfaces Inteligentes: Apesar da disseminação de interfaces gráficas (GUI), para muitas pessoas, os computadores continuam difíceis de usar. Por outro lado, à medida em que a população de usuários cresce e se diversifica as interfaces se tornam mais e mais complexas para acomodar hábitos e preferências variadas. Agentes de interface inteligentes poderiam, por exemplo monitorar as ações do usuário para desenvolver um modelo com suas habilidades e ajudá-lo automaticamente quando os problemas surgirem.

3. COMBATE CIBERNÉTICO

Como visto na seção anterior, a tecnologia de agentes pode resolver muitos problemas de diferentes formas. Em um primeiro momento aplicamos os agentes móveis para resolver o importuno problema dos ataques de negação de serviço (DoS ou DDoS) na transmissão em rede. Na rede, a largura da banda é um fator importante e algumas vezes um raro recurso de aplicação distribuída. A transação solicitada entre um cliente e um servidor pode requerer muitas voltas sobre a rede para ser completada. Este tipo de operação cria um tráfego muito grande e consome muito da banda de transmissão. Em um sistema sob ataque de hackers com muitos "clientes" e sistemas invadidos, o total de solicitações da bandas pode exceder a disponibilidade permitida, ocasionando uma performance muito ruim para as aplicações que estão envolvidas ou mesmo a parada total do sistema, configurando uma invasão do tipo DoS. Com a utilização de agentes para buscar as solicitações ou transações , enviando os agentes do cliente para o servidor, o fluxo na rede é reduzido. Desta maneira, somente o que os agentes encontrarem será transmitido pela rede, tornando a velocidade de transmissão maior. A arquitetura de agente projetada toma decisões sobre onde uma parte da funcionalidade pode residir, baseado no número de solicitações ao servidor, na banda de transmissão, no tráfego na rede, no número de clientes e servidores, dentre outros fatores.

Arquiteturas baseadas em agentes móveis são potencialmente muito menos suscetíveis a problemas de flexibilidade de ambientação do programa computacional. Algumas decisões devem ser feitas para melhorar o tempo gasto com desenvolvimento e o sistema é mais fácil de ser modificado depois de ser construído. Essa proposta de arquitetura de agentes, suporta adaptações da rede podendo fazer um novo desenho automaticamente. Este modelo de agentes também pode resolver problemas criados por intermitência ou má qualidade da conexão com a rede. Atualmente, algumas aplicações na rede são pesadíssimas para completar a transação ou obter localização de informação. Se, por exemplo, uma conexão cair, o cliente deve reiniciar a transação do ponto de partida. Com a tecnologia de agentes o cliente poderá obter as informações, mesmo que a conexão não esteja ativa, trabalhando off-line. Os agentes podem completar as transações e retornar os resultados para o cliente quando for restabelecida a conexão. Desta forma, a comunidade da inteligência artificial, tem lutado intensamente por mais de duas décadas e este potencial de aplicações é imensurável.

4. CONCLUSÕES E TENDÊNCIAS FUTURAS

Este trabalho apresenta um estudo de agentes que possuem mobilidade e comportamento inteligente. Ademais, foi desenvolvido uma arquitetura de agentes baseado em linguagem de programação PROLOG para realizar uma forma de monitoração e combate de invasões DoS e DDoS com o intuito de combatê-las de forma automática e sem necessitar a intervenção humana. Todavia, é preciso melhorar a interface e ampliar o escopo de atuação do agente inteligente móvel implementado. Agora, predizer qual será o papel dos agentes no futuro e como eles serão construídos, não é uma tarefa fácil. Entretanto, já existem várias aplicações baseadas em agentes que facilitam a vida dos usuários que usam redes de computadores, em destaque para Internet. Grandes universidades, centros de pesquisa e um número considerável de companhias, como a IBM e Microsoft, estão fazendo pesquisas na área de agentes inteligentes e o Departamento de Polícia Federal não pode ficar aquém a esta nova tecnologia.

5. BIBLIOGRAFIA

Nogueira, José Helano Matos. *Desenvolvimento de Sistemas Computacionais*. Editora ao Livro Técnico, janeiro, 2004.

Nogueira, José Helano Matos. *Ataques Cibernéticos*. Brasília: Revista Perícia Federal, Ano IV, Nº 13, páginas 23-28, janeiro/2003.

Nogueira, José Helano Matos. *Local de Crime na Internet*. Maceió: I Seminário Nacional de Perícia em Crimes de Informática, novembro/2002.

Nogueira, José Helano Matos. *Crimes de Alta Tecnologia.* I Congresso de Criminalística do Mercosul e IV Jornadas Latino-Americanas de Criminalística, Florianópolis, outubro, 2001.

Nogueira, José Helano Matos. *A Nova Face do Crime: Como Enfrentar e Prevenir a Ação dos HACKERS.* Brasília: Revista Perícia Federal, AnoIII, Nº 9, Julho 2001.

Nogueira, José Helano Matos. *Mipulator Robots Using Partial-Order Planning*. Springer Verlag, Advances in Artificial Intelligence, Lecture Notes in Artificial Intelligence, páginas 229 a 238, ISBN 3-540-65190-X, 1998.

Nogueira, José Helano Matos. *A Hybrid Formal Theory of Plan Recognition and Its Implementation*. Springer Verlag, Advances in Artificial Intelligence, Lecture Notes in Artificial Intelligence, páginas 31 a 40, ISBN 3-540-61859-7, 1996.

ALERTA: AS REDES SEM FIO CHEGARAM

José Helano Matos Nogueira

Perito Criminal Federal
Setor Técnico Científico
Departamento de Polícia Federal
SETEC/SR/DPF/CE
helano.jhmn@dpf.gov.br

ABSTRACT

With the continuous reduction of costs, wireless (WI-FI) will be each used time more, appearing new questions to be decided, as trustworthiness, easiness of installation, operation and mainly security; any intruder has relative easiness of invasion on this sort of net. This question has been sufficiently debated, but still they lack total adequate standards of security, and this work try to make an ALERT about this fact.

1. INTRODUÇÃO

A rede sem fio (Wireless) é um sistema de transmissão de dados flexível que pode ser utilizada como alternativa para as redes cabeadas. É uma tecnologia que permite a conexão entre equipamentos sem uma conexão física direta. O princípio de funcionamento das Wireless se baseia na transmissão de dados através da camada atmosférica utilizando a propagação das ondas eletromagnéticas, entretando o wireless engloba o uso de raios de luz infra-vermelha, apesar das ondas de rádio serem o meio mais difundido. Nos últimos anos esse tipo de rede tem crescido e tem ganhado popularidade nos diversos setores, principalmente no que diz respeito as WLAN (Wireless Local Area Network).

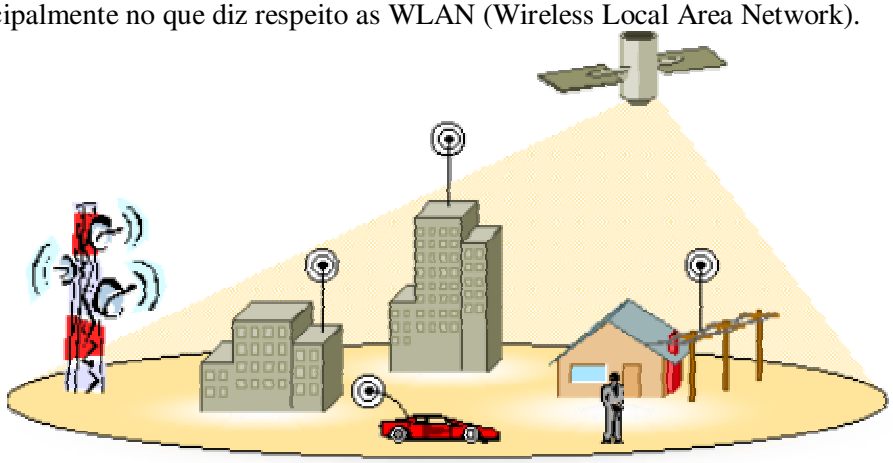


Figura 1 - Comunicação através de sinais de rádio

As redes *wireless*, também conhecidas como IEEE 802.11, Wi-Fi ou WLANs, são redes que utilizam sinais de rádio para a sua comunicação. Estas redes *wireless* ganharam grande popularidade pela mobilidade que provêem aos seus usuários e pela facilidade de instalação e uso em ambientes domésticos e empresariais, hotéis, conferências, aeroportos, dentre outros.

2. FUNCIONAMENTO

Wireless LANs (Redes de computadores Sem Fio)

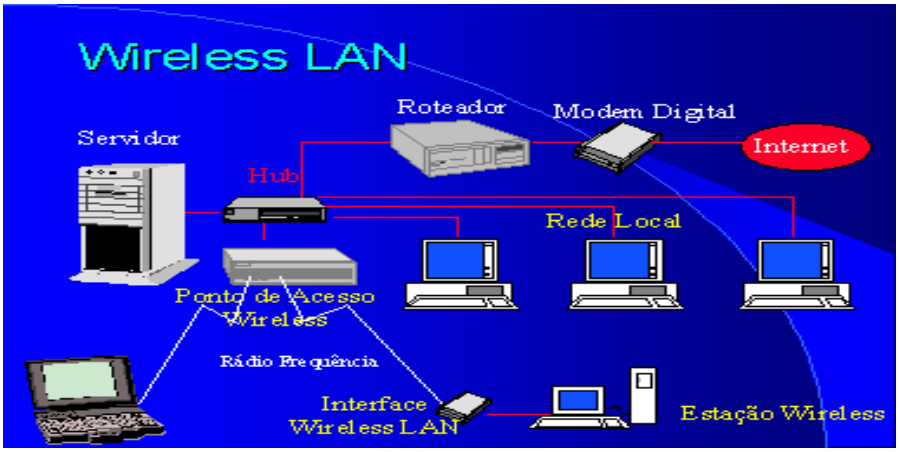


Figura 2 - Modelo de WLAN

Esta é uma das aplicações mais populares para a tecnologia wireless, em que se utiliza ondas de rádio para interligação de pontos de redes locais (LANs). Esta tecnologia permite que a rede vá para lugares onde as redes cabeadas não podem ir, desta forma usuários podem acessar informações compartilhadas e administradores de rede podem ajustar e gerenciar a rede sem se preocupar com instalações de cabos, outra vantagem é que a instalação das WLANs pode ser rápida e fácil eliminando a necessidade de se instalar uma quantidade muito grande de cabos internamente as paredes. Uma desvantagem é na Interligação de 2 redes locais (ponto-a-ponto), onde a sua maior limitação além da distância é a necessidade de se ter uma visada direta entre os 2 pontos, sendo como solução de contorno a utilização de repetidores no meio do caminho.

A questão principal sobre Wireless é a faixa de freqüência utilizada, pois são poucas as faixas que dispensam autorização prévia dos órgãos de controle de uso do espectro de freqüências (ex.: Anatel no Brasil, FCC nos EUA).

De acordo com a utilização do meio físico e da banda de freqüência assim como do tipo de mecanismo de modulação usado para transmissão as redes sem cabo podem ser definidas como *Banda Estreita* (Ondas de Radio, Microondas e Ondas Milimétricas, Infravermelho e Ondas Luminosas).

3. PADRÕES PARA REDES SEM FIO

Quando se discute a configuração de uma WLAN existem alguns padrões (desenvolvidos ou em desenvolvimento) que devem ser considerados:

IEEE 802.11: é o primeiro padrão firmado para redes sem fio. Apresenta suporte a WEP 5 e a implementação do sistema de rádio na banda ISM (*Industrial Scientifical Medical*) de 900 MHz.

Representa o primeiro padrão para produtos de redes locais sem fio, de uma organização internacionalmente reconhecida, a IEEE (*The Institute of Eletrical and Eletronics Engineers, Inc.*).

O padrão 802.11 possui diferentes versões:

- IEEE 802.11a [IEE99a]: é o padrão que descreve as especificações da camada de enlace lógico e física para redes sem fio. Segunda versão do padrão 802.11. Trabalha na freqüência de 5.8 Ghz. Disponibiliza 8 canais por ponto de acesso o que possibilita maiores taxas de transmissão para uma quantidade maior de usuários simultâneos.
- IEEE 802.11b [IEE99b]: descreve a implementação dos produtos WLAN mais comuns em uso atualmente. Este inclui aspectos da implementação do sistema de rádio e também inclui especificação de segurança. Esta descreve o uso do protocolo WEP. Trabalha na ISM de 2.4 GHz e prove 11 Mbps. Foi aprovado em julho de 2003 pelo IEEE.
- IEEE 802.11g [IEE03a][IEE03b]: descreve o mais recente padrão para redes sem fio. Atua na banda ISM de 2.4 GHz e provê taxas de transferências de até 54 Mbps. Integra-se a redes 802.11b e, assim como a 802.11a, suporta aplicações que fazem uso intensivo da largura de banda, apesar de ainda não ser um padrão utilizado.

- IEEE 802.11i [WiF03]: trata-se um grupo de trabalho que está ativamente definindo uma nova arquitetura de segurança para WLANs de forma a cobrir as gerações de soluções WLAN, tais como a 802.11a e a 802.11g.
- WPA [WPA02]: *Wi-Fi Protected Access*: é uma nova especificação da *Wi-Fi Alliance*. É baseada em torno de um subconjunto do padrão emergente IEEE 802.11i sendo desenhada para ser compatível com o mesmo, quando ele se tornar ratificado. Este padrão implementa o TKIP (T*emporal Key Integrity*) e tem como objetivo ser implementado em todos os dispositivos já concebidos através do *update* do *firmeware*.

4. VANTAGENS DA REDE SEM FIO (WIRELESS)

Redes sem fio oferecem as seguintes vantagens financeiras, de produtividade e de conveniência, sobre as tradicionais redes fixas:

• Mobilidade - Sistemas de redes locais sem fio podem providenciar aos usuários acesso à informação em tempo real em qualquer lugar de suas organizações.

• Instalação rápida e simples - Instalar uma rede local sem fio pode ser rápido e fácil, além de eliminar a necessidade de atravessar cabos através de paredes e andares.

• Flexibilidade -Tecnologia sem fio permite que as redes cheguem aonde cabos não podem ir.

• Custo Reduzido- Enquanto que o custo inicial de uma rede local sem fio pode ser maior que de uma rede local fixa, a instalação e o ciclo de vida são significantemente mais rápidos.

• Escalabilidade - Redes locais sem fio podem ser configuradas segundo diversas topologias de acordo com as necessidades. Configurações podem ser mudadas facilmente e a distancia entre as estações adaptadas desde poucos usuários até centenas.

5. DESVANTAGENS DA REDE SEM FIO (WIRELESS)

Uma desvantagem da tecnologia sem fio é a segurança. Ao contrário das redes cabeadas, onde a infra-estrutura fica dentro das corporações, as redes sem fio usam ondas de rádio como meio de transmissão, o que aumenta as chances de acessos não autorizados.

Uma das ameaças é o chamado warchalking, termo que designa os símbolos comuns entre os hackers para indicar que em determinado lugar existe vulnerabilidade de acesso. A cultura dos warchalking começou a ser disseminada em Londres e as calçadas foram escolhidas como ponto de referência para a marcação dos símbolos.

Para qualquer executivo de TI ter na frente de sua corporação algum destes sinais deve tomar as devidas providências o quanto antes. O sistema desenvolvido pelos hackers é simples: com um notebook que possui a interface Wi-Fi, ou seja, apresenta interoperabilidade com a tecnologia de WLAN, e um programa como o AirSnort, eles captam as informações para estabelecer uma conexão com a rede sem fio da empresa atacada.

As soluções disponíveis no mercado utilizam em sua maioria o padrão WEP para garantia de sigilo das informações. O WEP ou Wired Equivalent Privacy, que utiliza a implementação do protocolo RC4 para realizar criptografia, já mostrou sinais de falhas graves. Pesquisadores descobriram que era possível ter acesso à chave utilizada na criptografia provocando o surgimento de diversas ferramentas para quebra do WEP na Internet.

Contar com o WEP, que está disponível na maior parte dos equipamentos wireless, está longe de ser garantia para a segurança dos dados transmitidos.

Além do WEP, não se pode dispor das demais características de segurança disponíveis em Access Points e interfaces de rede. Controle de acesso por endereços MAC e comunidades SNMP são alguns exemplos de funcionalidades que podem ser burladas. E isso não é suficiente.

6. TIPOS DE ATAQUES

Os ataques às redes sem fio não são novos. Ao invés disso, eles são baseados em ataques anteriormente descobertos em redes guiadas. Alguns destes ataques não sofreram nem uma

modificação, já outros sofrem algumas modificações para que possam ser disparados e obter melhores resultados.

Na realidade, o objetivo dos ataques não é comprometer a rede sem fio, mas sim ganhar acesso ou comprometer a rede guiada.

Como as redes guiadas tradicionais tem sido duramente atacadas durante mais de trinta anos, muitas desenvolveram excelentes defesas. Por exemplo, o uso de um *firewall* propriamente configurado pode aumentar sensivelmente o nível de segurança da instituição. Entretanto, se esta mesma instituição possuir uma rede sem fio mal configurada atrás deste *firewall*, é como se existisse um *backdoor* devidamente instalado.

Atualmente, a maioria das WLANs irão certamente sofrer de pelo menos um tipo de ataque. Estes ataques não são limitados a instituições, visto que o maior número de equipamentos deste tipo de rede é vendido para consumidores domésticos. Os quais procuram aumentar sua largura de banda ou distribuir sua conexão em toda sua residência.

- Associação Maliciosa

A associação maliciosa ocorre quando um atacante passando-se por um *access point*, ilude outro sistema de maneira a fazer com que este acredite estar se conectando em uma WLAN real.

- ARP Poisoning

O ataque de envenenamento do protocolo de resolução de endereços (ARP) é um ataque de camada de enlace de dados que só pode ser disparado quando um atacante está conectado na mesma rede local que a vitima. Limitando este ataque às redes que estejam conectadas por *hubs, switches* e *bridges.* Deixando de fora as redes conectadas por roteadores e *gateways*.

- MAC Spoofing

Existem muitas instituições que criam listas de acesso para todos os dispositivos explicitamente permitidos à conexão. Estas instituições costumam fazer este controle através do endereço MAC da placa do cliente. Banindo desta forma o acesso de outras placas não autorizadas. Entretanto, os dispositivos para redes sem fio possuem a particularidade de permitir a troca do endereço físico. Com isso, atacantes mal intencionados podem capturar através de técnicas de *Eavesdrooping & Espionage* um endereço MAC válido de um cliente, trocar seu endereço pelo do cliente e utilizar a rede. Além deste tipo de *MAC Spoffing*, existe o *MAC Spoffing* da placa de rede guiada dos *access points.*

- Ataques de Vigilância

Ataque de vigilância, apesar de não ser considerado ataque para muitos estudiosos, pode se tornar um ataque com um grau de comprometimento muito grande dependendo da finalidade para a qual este ataque é efetuado. A idéia por trás deste ataque é encontrar fisicamente os dispositivos de redes sem fio para que estes dispositivos possam, posteriormente, ser invadidos. Podendo ainda ter sua configuração *resetada* à configuração padrão ou ainda ser roubado. No caso em que um *access point* pode ser *resetado*, um atacante pode invadí-lo, conseguindo gerar ataques dentro da porção guiada da rede. Representando assim um grande risco a exposição de equipamentos.

- Wardriving

Wardriving é uma forma de ataque muito parecida com a anterior. Modifica-se somente a forma de como as WLANs são encontradas. Utilizam-se neste tipo de ataque equipamentos configurados para encontrar tantas redes sem fio quantas aquelas que estiverem dentro da área de abrangência do dispositivo de monitoramento. O objetivo deste tipo de ataque, além dos já mencionados nos ataques de vigilância é mapear todos os *access points* encontrados com o auxilio de um GPS (*Global Position System*).

- Warchalking

Este tipo de ataque tem como objetivo encontrar redes sem fio através de técnicas de *wardriving* e marcar estas redes através da pichação de muros e calçadas com símbolos específicos. Isto para que outros atacantes possam de antemão saber quais as características da rede. Existem grupos organizados para *warchalking* que se utilizam símbolos próprios para marcar as redes numa tentativa de mantê-las em segredo. Existem também grupos rivais que tentam encontrar e pichar o maior número de redes possível para ganhar mais status.

7. VULNERABILIDADES

As redes sem fio tornaram-se alvo de exaustivos estudos e muitos ataques foram desenvolvidos e/ou adaptados para poderem se valer das fraquezas presentes nestas redes. Além disso, estas redes apresentam falhas graves de segurança e problemas na implementação e conceituação do próprio protocolo.

Um fator importante relacionado à segurança de redes sem fio é o fato de que os ataques gerados dentro destas redes são disparados dentro do mesmo domínio de colisão. Ou seja, o atacante se comunica com o mesmo concentrador de tráfego do sistema o qual almeja atacar.

8. PONTOS VULNERÁVEIS NO PROTOCOLO

O protocolo 802.11 em si é bem conciso e insere inúmeras novidades. Por ser um protocolo devidamente estudado, não possui um grande número de vulnerabilidades. Entretanto, as poucas que possui pode trazer grandes problemas à rede como um todo.

Uma vulnerabilidade em evidência hoje diz respeito à criptografia WEP.

Outra vulnerabilidade encontrada, além de pacotes *beacon frames* com características peculiares, trata-se das formas de autenticação permitidas no protocolo.

8.1. Vulnerabilidades do WEP

O protocolo WEP, é incorporado como uma parte do 802.11b. A implementação do protocolo WEP, que utiliza-se da criptografia RC4, possui algumas vulnerabilidades. Devidas à forma de implementação utilizada.

Vulnerabilidades nas formas de autenticação

Os access points , podem permitir a autenticação aberta.

Este tipo de autenticação permite que qualquer dispositivo que saiba qual o SSID da WLAN em questão possa se associar. Apesar de garantir a facilidade de conexão entre um cliente e um access point, esta forma de autenticação faz com que seja feito o broadcast da conexão guiada na rede sem fio, seria como colocar um *hub* em um local público, onde qualquer pessoa pode se conectar livremente.

Beacon Frames

Devidamente especificado no protocolo 802.11. Um beacon frame é um frame de sinalização e sincronismo, além de enviar informações importantes a respeito do funcionamento da rede sem fio em questão. Access points a princípio são configurados de maneira a enviar beacon frames no canal em que atuam, bem como no canal subseqüente e antecessor.

Rogue WLANs

Chamadas de WLANs grampeáveis, são instaladas na maioria das vezes sem o consentimento da instituição, portanto não seguindo a política de segurança.

Estas redes podem ser facilmente escondidas da rede guiada com a duplicação do endereço MAC da máquina anteriormente ligada àquele ponto.

Configurações Inseguras

Muitas instituição aumentam o nível de segurança de suas WLANs com a utilização de VPNs e erroneamente acreditam que esta se torna à prova de invasões. Deixando de lado as configurações de segurança dos dispositivos da rede sem fio.

Entretanto, um hacker mais experiente, ao invés de tentar quebrar a VPN, acaba atacando os dispositivos para redes sem fio como, por exemplo, um acess point ou um cliente.

Associação Acidental

Muitos dos sistemas operacionais costumam configurar automaticamente os dispositivos para redes sem fio. Com o barateamento da tecnologia, a integração desta tecnologia em computadores pessoais, como notebooks, torna-se inevitável. Isso faz com que pessoas leigas desconheçam a existência deste dispositivo. Outro fator importante é que mesmo sabendo da existência do dispositivo estas pessoas não sabem ao certo como configurar, manipular e gerenciá-lo. Assim sendo, existe uma grande possibilidade deste dispositivo se associar a outro dispositivo, sem o consentimento ou mesmo conhecimento do usuário.

Um simples exemplo de como esta associação pode ocorrer esta relacionada a duas empresas A e B. Ambas possuem clientes e redes sem fio. Se o sinal da rede B invadir o campo de abrangência da rede A um cliente da rede A pode se associar acidentalmente à rede B. Além disso os access points de A podem se associar aos access points de B e criar uma ESS.

8.2. Riscos Externos

Nos riscos externos, diferentemente dos internos, é exigida a interação direta dos atacantes para expor as vulnerabilidades.

Eavesdropping & Espionage

Este risco é muito parecido com o existente nas redes guiadas dos sniffers .O objetivo dos dois é o mesmo: Conseguir capturar e analisar todo o tráfego que passa pela rede. Utilizando os dados obtidos para gerar possíveis ataques ou roubar informações e senhas.

Entretanto, para que um atacante consiga obter o tráfego nas redes guiadas é necessário que este esteja dentro do mesmo domínio de colisão que a rede a qual deseja obter os pacotes. Ou seja, é necessário que o atacante tenha controle de pelo menos uma máquina ligada fisicamente à rede que pretende atacar.

Roubo de Identidade

O roubo de identidade ocorre quando um atacante consegue obter tantas informações quanto necessárias para poder se passar por um cliente válido da WLAN.

Muitas WLANs fazem a filtragem por endereços MAC. Com isso, mesmo que um atacante conheça o SSID da rede e saiba que a autenticação é aberta ele não consegue se associar à WLAN. O mesmo ocorre quando a WLAN não disponibiliza serviços de DHCP.

Então, para que o atacante possa usufruir a rede é necessário que ele obtenha um endereço MAC válido, bem como, um endereço IP também válido, conseguindo assim acesso a rede.

8.3. Mecanismo de proteção em redes Wireless

Para se obter um nível de segurança satisfatório é preciso implementar controles externos aos equipamentos. Configuração adequada, criptografia, autenticação forte e monitoração dos acessos da rede sem fio são imprescindíveis.

A solução para segurança de redes wireless é dividida nas seguintes fases e atividades:

Análise do Ambiente

Nesta fase o ambiente é analisado e a localização de pontos de acesso e antenas é constatada. São realizadas verificações quanto ao alcance da rede através de ferramentas de análise do sinal transmitido. O objetivo é checar se a rede pode ser acessada fora dos perímetros da corporação.

Especificação e Configuração dos Equipamentos

As necessidades de segurança observadas nesta fase serão especificadas, seguidas da melhor configuração dos equipamentos. Configurações estas, onde se pode incluir características de segurança personalizadas. Pois, mesmo não sendo confiáveis se utilizadas isoladamente, constituem mais uma barreira a ser vencida quando utilizada em conjunto com os demais itens da solução exposta. A especificação de soluções para as necessidades de segurança observadas será realizada em conjunto com a configuração adequada dos equipamentos. Durante as configurações são incluídas as características de segurança disponíveis nos equipamentos. Mesmo não sendo confiáveis se utilizadas isoladamente, constituem mais um perímetro de segurança a ser vencido quando utilizada com os demais itens da Solução exposta.

Implementação de Criptografia

É fundamental o uso de criptografia confiável uma vez que não é possível contar com o WEP. Durante esta etapa a implementação de uma VPN na rede sem fio é realizada utilizando recursos já existentes ou utilizando soluções de mercado.

Autenticação Forte

Para controlar o acesso aos recursos disponibilizados através de uma rede wireless é fundamental utilizar autenticação forte. Contando com o legado do cliente observado na fase de especificação ou aplicando novas soluções, é implementado controle de acesso com tecnologias líderes e amplamente utilizadas no mercado.

Monitoração

Os acessos aos Access Points instalados e a rede propriamente dita devem ser monitorados. Mesmo com a utilização de criptografia é possível, e necessário, monitorar os acessos realizados. A monitoração é seguida do envio de alertas, previamente configurados.

9. FERRAMENTAS PARA SEGURANÇA REDES SEM FIO

NetStumbler (http://www.netstumbler.com)
Kismet (http://www.kismetwireless.net)
Wellenreiter (http://www.wellenreiter.net)
Ethereal (http://www.ethereal.com)
AirSnort (http://airsnort.shmoo.com)
HostAP (http://hostap.epitest.fi)
Orinoco/Wireless Tools (http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html)

SANS INTERNET STORM CENTER – DETECÇÃO DA NOVA TENDÊNCIA DE CRIAÇÃO DE MALWARES

Pedro Paulo F. Bueno

SANS Internet Storm Center Incident Handler

Abstract

Over the last few years, the security community has been observing a new movement related to malware: Malware development is accelerating due to efficient and open collaboration, moving from months and years to weeks and days.

In this paper, we will present an overview of this new development and illustrate it using case studies of recent malware. Our examples include AGO/GOA/Phatbot variants, as well as the recent Sasser worm.

In this way, it will be possible to illustrate how the SANS Internet Storm Center and the Incident Handlers can help the initial detection and watch these worms, looking for ways to mitigate the effects and alerting the internet community in a responsible and efficient way.

1. HISTÓRICO

O Internet Storm Center [1] é um projeto do The SANS Institute [2], criado a partir do SANS Institute Consensus Database (CID), que visa à monitoração do tráfego global da Internet, desde Novembro de 2000. Após o advento do worm Lion [3], em Março de 2001, detectado com sucesso pelo CID, em que toda a tecnologia, as pessoas e os dados que possibilitaram a detecção do Lion eram do SANS, o CID ganhou um novo nome, Internet Storm Center (ISC).

Atualmente o ISC recebe mais de 3.000.000 de logs de Intrusion Detection Systems (IDS), firewalls e routers espalhados por todo o globo. Através de uma detecção correlacionada dos dados, é possível uma ação mais rápida em cima dos incidentes, isolando sites utilizados pelos intrusos.

O ISC conta ainda com cerca de 30 Incidents Handlers, pertencentes a grandes provedores mundiais, agencias civis e militares e institutos de segurança, que são os responsáveis por analisar os dados e informações recebidas diariamente e que ajudam a compor o editorial diário, chamado Handler's Diary.

2. INTRODUÇÃO

A ultima leva de worms que atingiu a Internet em 2004 trouxe algo de novo em relação aos seus antecessores: o rápido desenvolvimento a partir de uma vulnerabilidade descoberta.

Teoricamente, o fluxo comum da criação de um worm é composto de 3 fases, vistas a seguir:

Liberação por parte do fabricante ou grupos de pesquisa em segurança, das vulnerabilidades nos softwares. O recomendado e observado atualmente é que na maioria das vezes temos a liberação das informações das vulnerabilidades juntamente com as correções necessárias para se evitar possíveis problemas de exploração das mesmas;

Implementação dos PoC (Proof of Concept) demonstrando a exploração da vulnerabilidade. Os exploits podem ser distribuídos publicamente, via websites [5] ou listas de discussão [6];

Desenvolvimento de aplicações automatizadas que explorem a vulnerabilidade remota, instalem seu código malicioso e, entre outras coisas, comece a realizar scanning em busca de novos hosts que possam estar vulneráveis e então explorar novamente a vulnerabilidade.

A seguir veremos dois exemplos de detecção de worms que servem para ilustrar o exemplo da nova tendência observada. A titulo de comparação, o primeiro exemplo será o worm Slammer, lançado em 25 de Janeiro de 2002. Posteriormente veremos o worm Sasser, lançado no dia 1º de Maio de 2004 e a família de variantes AGO/GOA/Phatbot.

3. DETECÇÃO DE WORMS

Com todo o tráfego recebido pelo ISC é possível traçar certas características do worm que torna possível a identificação antes mesmo dele começar a se propagar. Abaixo temos dois exemplos distintos. Primeiro observaremos o tráfego relacionado à porta 445, utilizado mais recentemente pelo Worm Sasser, e em seguida, o tráfego da porta 443, não explorado por nenhum worm mais recente. Ambos os gráficos abaixo se referem a dados do Internet Storm Center, datados de 19 de abril a 26 de maio de 2004.

3.1. Porta 445

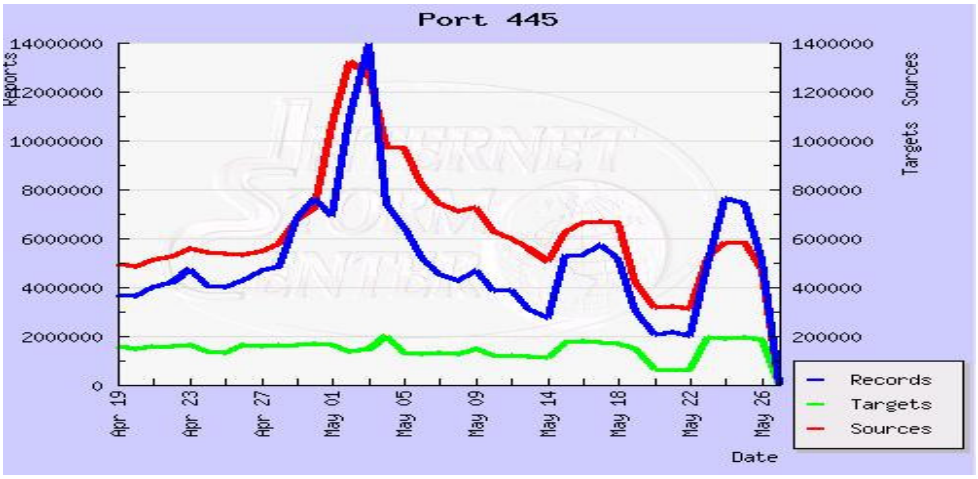


Figura 1: Tráfego da porta 445 / Fonte: ISC

Na figura acima podemos observar que o numero de IPs de origem está em crescimento estável com um súbito crescimento no dia 1º de Maio, indicando que muitos IPs diferentes começaram a realizar scannings buscando pela porta 445. Dia 1º de Maio, como veremos a seguir foi o dia do surgimento do Worm Sasser.

3.2. Porta 443

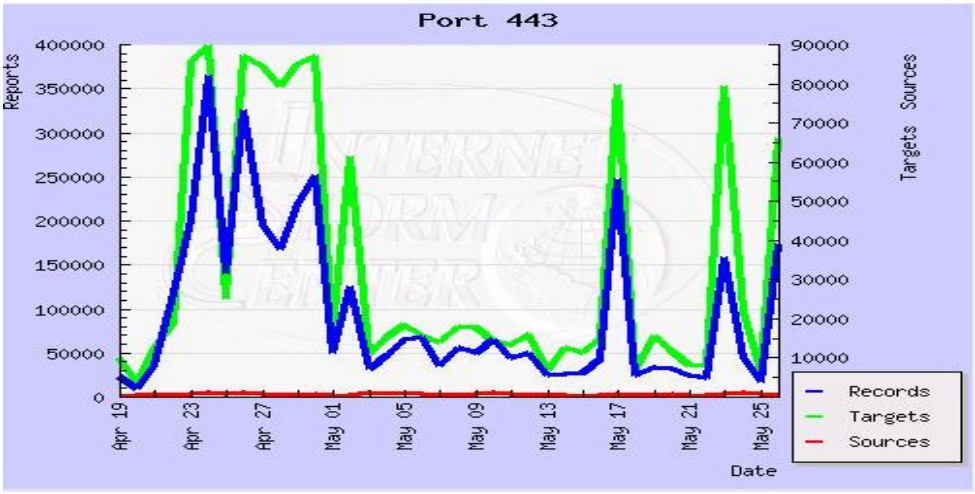


Figura 2: Tráfego da Porta 443 / Fonte: ISC

A figura 2 mostra o tráfego recente relacionado à porta 443. Nesta figura podemos observar que apesar do numero de alvos (targets) ser alto, o número de endereços de origem é baixo, indicando que se trata de um grande scan a procura de portas 443 abertas, mas realizado por poucas origens distintas, quando comparado com o volume de alvos. As razões desse scanning podem ser diversas, desde a procura de servidores que utilizem versões de OpenSSL recentemente descobertas como vulneráveis [9], ou em busca de servidores IIS descritos como vulneráveis de acordo com o Microsoft Security Bulletin MS04-011 [10]

4. CASO DE ESTUDO 1: SLAMMER

No dia 25 de Janeiro, as redes mundiais começaram a sentir os efeitos do worm Slammer, chegando a ponto de varias redes perderem a conectividade devido ao tráfego causado por ele. O Slammer possui ainda hoje alguns números impressionantes:

- Nos primeiros 3 minutos após seu aparecimento, realizava cerca de 55 milhões de scannings por segundo;
- Era capaz de dobrar o numero de infecções a cada 8.7 segundos;
- Em 10 minutos atingiu cerca dos 90 % dos hosts vulneráveis;

4.1. O MS-SQL

O Microsoft SQL Server utiliza basicamente duas portas principais. A mais usada é a porta 1433, baseada em TCP, utilizada para responder a queries e para transferência de dados. A segunda é a porta 1434, baseada em UDP, chamada de SQL Server Resolution Service, utilizada pelo cliente para identificar os métodos de conexão disponíveis.

4.2. A Vulnerabilidade

De acordo com o Common Vulnerabilities Exposure Database (CVE) [7]:

"Multiple buffer overflows in SQL Server 2000 Resolution Service allow remote attackers to cause a denial of service or execute arbitrary code via UDP packets to port 1434 in which (1) a 0x04 byte causes the SQL Monitor thread to generate a long registry key name, or (2) a 0x08 byte with a long string causes heap corruption."

4.3. A Cronologia do Worm Slammer

A cronologia do worm Slammer ilustra o ponto que iremos mostrar posteriormente, sobre o encolhimento nos prazos de desenvolvimento de worms. Vejamos algumas datas importantes do Slammer:

- 24 de Julho de 2002 : A Microsoft liberar o Security Bulletin MS02-39 referente a vulnerabilidade no MS-SQL Server;
- Novembro de 2002 : O 1º exploit relacionado a vulnerabilidade do MS-SQL Server é publicamente conhecido, postado no site packetstormsecurity.com;
- 24/25 de Julho de 2003: ´Slammer Day!´

4.4. Slammer e o SANS Internet Storm Center

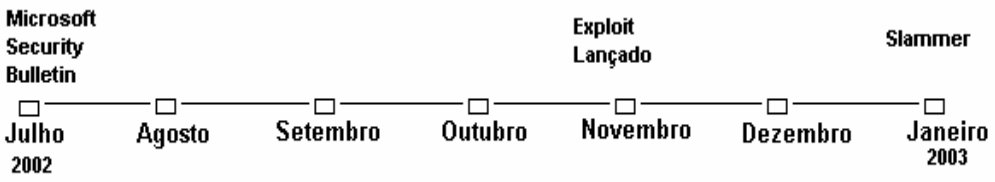
Nos dias anteriores ao Slammer, alguma atividade já havia sendo notada pelo ISC, como probes por portas 1434, porem esse numero era constante, e o principal indicador de worm não aparecia, o numero de 'source ips' continuava estático. No dia 25 de Janeiro, essa situação se modificou, com o numero de 'source ips' crescendo de uma forma totalmente inesperada.

A essa altura, com a detecção de pacotes por varias fontes diferentes, o website do Internet Storm Center, já constava com os dados relativos aos acontecimentos, alem de exemplos dos pacotes do Slammer, formas de mitigação, e assinaturas de IDS que poderiam ser utilizadas para identificar possíveis focos de infecção.

Devido a alguns fatores como sua rápida propagação, redes indisponíveis, fácil eliminação através do reinicio da maquina, e ainda, fácil mitigação, através de filtros ingress e egress para porta 1434, o segundo dia após seu aparecimento foi bem mais calmo que o primeiro, com o numero de hosts infectados diminuindo rapidamente.

4.5. Slammer – Conclusão

Sem considerar os dados do Slammer, em relação aos prejuízos causados, devemos nos focar no ponto principal para nosso artigo: Desde o lançamento oficial da vulnerabilidade por parte da Microsoft, através do Security Bulletin, até o primeiro exploit, temos 4 meses, e mais 2 meses até o aparecimento do worm.



5. CASO DE ESTUDO 2: WORM SASSER

O worm Sasser foi um worm que explorava uma vulnerabilidade no serviço LSASRV do sistema operacional Windows.

5.1. O worm Sasser

No dia 1º de maio de 2004, o Sasser começou a se espalhar infectando maquinas que não haviam aplicado o patch do Microsoft Security Bulletin MS04-011, o qual continha a correção para o serviço RPC/LSASS, explorado pelo Worm.

Estima-se que o Sasser tenha atingido um numero entre 600 e 800 mil hosts.

Ao infectar uma maquina via porta 445, ele abre um Shell remoto na porta 9996 e em seguida utiliza essa porta para fazer um ftp na porta 5554 da maquina que o infectou, para baixar o binário do worm a ser executado na vitima.

5.2. A Vulnerabilidade

De acordo com o Common Vulnerabilities and Exposures Database (CVE) [8]:

"Stack-based buffer overflow in certain Active Directory service functions in LSASRV.DLL of the Local Security Authority Subsystem Service (LSASS) in Microsoft Windows NT 4.0 SP6a, 2000 SP2 through SP4, XP SP1, Server 2003, NetMeeting, Windows 98, and Windows ME, allows remote attackers to execute arbitrary code via a packet that causes the DsRolerUpgradeDownlevelServer function to create long debug entries for the DCPROMO.LOG log file, as exploited by the Sasser worm."

5.3. A Cronologia do Worm Sasser

A Cronologia do Sasser mostra algo bem diferente do observado em relação ao Slammer:

Observemos as datas [4]:

- 13 de Abril – A Microsoft lança o conjunto de correções para seus sistemas operacionais. Entre as correções, temos no pacote MS04-011 uma correção para o serviço RPC/LSASS que pode ser explorado remotamente;
- 14 de Abril – Exploit para DoS no IIS;
- 21 de Abril – Exploit para SSL no IIS;
- 25 de Abril – O Exploit para explorar remotamente o serviço LSASS é lançado publicamente;
- 27 de Abril – A família de worms AGO/GAO/Phatbot começa a testar o exploit em sua base de conhecimento de exploits visando infectar mais maquinas;
- 30 de Abril/1º de Maio – ´SASSER Day!´;
- 02 de Maio – 1ª variante do Sasser;

Entre o anuncio oficial da Microsoft sobre a vulnerabilidade, juntamente com as correções, e o inicio do worm, temos apenas 17 dias, contra 6 meses do Slammer.

5.4. Sasser e o Internet Storm Center

Desde o lançamento do pacote de correções pela Microsoft, o ISC já começou a monitorar as possíveis conseqüências do mesmo. Já se esperava uma série de exploits, devido ao volume de correções liberado pela Microsoft, e isso foi acontecendo aos poucos, primeiramente com o lançamento de exploits visando o SSL, e posteriormente com o lançamento público do exploit para o RPC/LSASS.

6. AGO/GOA/PHATBOT

6.1. Funcionamento

A família de variantes dos vírus/worms AGO/GOA/Phatbot representa uma verdadeira revolução em relação ao desenvolvimento de novos worms na Internet.

Primeiramente, ele busca comprometer as maquinas pelo maior numero de tentativas possíveis através de uma base de exploits [11], como por exemplo, DCOM/RPC, WebDav, UpnP e outras, não importando se são novas ou antigas, e com isso tentando atingir várias portas diferentes, como portas abertas por vírus, como MyDoom, ou de serviços, como os citados anteriormente.

A família AGO/GOA/Phatbot possui dois mecanismos distintos para controle das maquinas infectadas. Para o AGObot o mecanismo escolhido foi via IRC. Ou seja, quando ele conseguia infectar uma maquina, ele se conectava a uma rede de IRC em um canal especifico, pelo qual poderia receber os comandos de controle da maquina, tudo de forma remota.

No caso do Phatbot [13] foi escolhido um mecanismo de Peer-to-Peer, (P2P) para o controle.

6.2. Desenvolvimento

Talvez o mecanismo que contribua mais para a disseminação da família AGO/GOA/Phatbot seja a cooperação no seu desenvolvimento. Conforme já suspeitado devido o alto numero de variações, o código fonte desses bots já estava circulando entre os hackers à alguns tempo, chegando ao ponto de conter em seu código, referencias ao modelo GNU de licenciamento Open Source [14].Isso possibilitou que cada pessoa pudesse alterar o código e inserisse sua própria base de exploits, criando uma nova variante.

6.3. Família AGO/GOA/Phatbot e o Worm SASSER

Conforme observado nos reports diários do SANS, o Handler's Diary [11], primeiramente foram observados aumentos em atividades de algumas portas, já conhecidas e utilizadas pela família AGO/GOA/Phatbot, e um aumento de atividade na porta 445, o que poderia significar a utilização do exploit pelos bots. Ainda de acordo com analise realizada posteriormente e publicada no handler's diary do dia 04 de maio [12], o tráfego observado anteriormente ao Sasser se devia a uma das variantes dos AGO/GOA/PhatBot testando a inclusão do exploit do RPC/LSASS dentro da sua base de conhecimento de exploits.

Por isso, poucos dias antes do real surgimento do Sasser, já havia um prenuncio de que algo no gênero iria aparecer, fosse pela família de AGO/GOA/Phat, fosse por um worm dedicado.

7. PRÓXIMOS PASSOS...?

Os próximos passos nesse caso não seriam muito complicados de se prever, no caso do worm Sasser, ele derivou na criação de outro worm, chamado Dabber [15], que, ironicamente, explorava uma vulnerabilidade no código do servidor FTP instalado pelo Sasser.

Essa nova tendência de cooperação aberta por parte dos fabricantes de malware pede também uma rápida ação tanto dos fabricantes de Anti-virus correndo contra o tempo para identificar e criar vacinas eficientes, quanto do usuário final/administradores, em atualizar as maquinas, sistemas operacionais e serviços para evitar futuros ataques, sejam eles praticados por hackers ou worms.

O SANS Internet Storm Center está aberto para consultas relacionadas a tráfego a qualquer porta, mostrando um histórico que possibilite que se detecte uma nova tendência, como o scanning por um serviço que possua uma vulnerabilidade ainda não pública. Além disso, o grupo de Incident Handlers do ISC está pronto para receber qualquer tráfego ou malware suspeito para ajudar a identificar a ameaça e possibilitar que se possam mitigar futuros incidentes de segurança.

8. REFERENCIA BIBLIOGRÁFICAS

1 – SANS Internet Storm Center – http://isc.sans.org
2 – The SANS Institute – http://www.sans.org
3 – SANS Institute – Lion Worm - http://www.sans.org/y2k/lion.htm
4 – SANS Webcast Achieve - http://www.sans.org/webcasts/show.php?webcastid=90488
5 – K-otik WebSite – http://www.k-otik.com
6 - Full-Disclosure Mailing List
7 - Common Vulnerabilities Exposure - http://cve.mitre.org - CVE – CAN2002-0649
8 - Common Vulnerabilities Exposure - http://cve.mitre.org - CVE – CAN2003-0533
9 – Common Vulnerabilities Exposure - http://cve.mitre.org - CVE – CAN2004-0079, CAN2004-0081, CAN2004-0112
10 - Common Vulnerabilities Exposure - http://cve.mitre.org - CVE CAN-2003-0719

11 – SANS ISC Handlers Diary - http://isc.sans.org/diary.php?date=2004-04-24
12 – SANS ISC Handlers Diary - http://isc.sans.org/diary.php?date=2004-04-18
13 – LURHQ PhatBot Analysis - http://www.lurhq.com/phatbot.html
14 – F-Secure Weblog Archives - http://www.f-secure.com/weblog/archives/archive-042004.html
15 – LURHQ Dabber Analysis - http://www.lurhq.com/dabber.html

NECESSIDADES E DESAFIOS PARA DEFINIÇÃO DE UMA METODOLOGIA PARA PROTEÇÃO DA INFRA-ESTRUTURA CRÍTICA DE TELECOMUNICAÇÕES

Edson Kowask Bezerra, Emilio Tissato Nakamura,

Marcelo Barbosa Lima, Sérgio Luís Ribeiro

CPQD - Centro de Pesquisa e Desenvolvimento - Telecom & IT Solutions
Rod Campinas – Mogi-Mirim, km 118,5 – SP340 – CEP 13086-902 – Campinas/SP
{kowask, nakamura, mlima, sribeiro}@cpqd.com.br

Abstract

The main objective of this article is to show the challenges and motivations to create a plan to protect the telecommunications´ critical infrastructure and the reason for Brazil should do it. This topic represents a reality that all the countries are facing: creating a methodology to protect the infrastructure, the countries are concerned about that, and some of them are working seriously on that since early 2000.

Palavras-Chaves: proteção da infra-estrutura crítica de telecomunicações, segurança em telecomunicações, contexto internacional, metodologia de proteção a infra-estrutura crítica de telecomunicações.

1. INTRODUÇÃO

A natureza dos riscos e as vulnerabilidades na infra-estrutura crítica de telecomunicações têm se tornado um tema cada dia mais em evidência nas mídias nacionais e internacionais. De fato antes dos anos 80 não existia tanta repercussão sobre esse assunto. Existiam poucas motivações, com pouca ênfase e pouca seriedade sobre o assunto. Mas após a identificação do *bug* do milênio muita coisa mudou.

Foi nessa época que a humanidade percebeu o quanto ela estava vulnerável e dependente da informação. Com isso os países começaram a se movimentar e a criar grupos de estudos e pesquisas para tratar do assunto. Mas, apesar de todo esforço, a cultura de segurança ainda era muito pequena. Foi necessário um outro incidente grave de segurança, como os atentados terroristas de 11 de Setembro de 2001 para que as nações efetivamente aumentassem os investimentos e criassem grupos para estudar e oferecer um plano de segurança da infra-estrutura crítica de telecomunicações.

Este artigo tem como principal objetivo mostrar quais são as motivações e dificuldades encontradas na criação de um modelo e de uma metodologia para proteção da infra-estrutura crítica de telecomunicações no Brasil. Além disso, o artigo discute como a maioria dos outros países está tratando esse tema.

Com todos esses embasamentos, será possível, num futuro próximo, identificar qual a situação atual do Brasil e traçar planos e delinear um cenário ideal onde a infra-estrutura de telecomunicações seja mais segura, garantindo assim, uma maior estabilidade e continuidade dos serviços de telecomunicações no Brasil em ocasiões adversas.

2. MOTIVAÇÃO

Todas as infra-estruturas de um país são críticas em sua essência, mas o grande desafio está em determinar o nível de criticidade de cada infra-estrutura, para que as ações possam ser priorizadas.

É sabido que todas as infra-estruturas críticas são vitais ao país, sejam elas, energia, água e esgoto, sistemas vitais da sociedade (saúde, segurança e bem estar público) financeiro, administrativos, etc. Caso uma dessas infra-estruturas seja afetada total ou parcialmente, enormes prejuízos são causados ao país, seja no âmbito financeiro, político ou social.

A definição de qual infra-estrutura possui mais vulnerabilidades envolve um aprendizado constante, no qual a evolução e o conhecimento possuem um papel primordial. Partindo do pressuposto que se temos uma infra-estrutura e essa é mais antiga, por conseqüência ela é mais conhecida e a sua técnica é bastante dominada. Com isso, as vulnerabilidades e riscos são mais conhecidos o que cria a possibilidade deles serem eliminados, mitigados ou assumidos. Então, uma infra-estrutura mais nova pode ser considerada menos conhecida, sua técnica menos dominada, e portanto as vulnerabilidades e riscos ainda não são totalmente conhecidos. Isso faz com que essa infra-estrutura se torne mais vulnerável e propensa a sofrer algum incidente de segurança.

Isso pode ser amplamente demonstrado pelo fato de que as maiorias das infra-estruturas (antigas) já passaram por alguma situação adversa, seja por uma guerra, ataque, blecaute, greve, fraude, dimensionamento errôneo, etc. Essas dificuldades criaram uma cultura nas instituições, empresas e governos de como lidar com essas situações. Um exemplo clássico e bem recente foram os problemas ocorridos nas infra-estruturas de energia elétrica do Brasil em 2003, que fizeram com que a maioria das empresas, tanto no setor privado como público criassem fontes redundantes de energia, os Governos, os Estados e até os cidadãos mudaram seus hábitos, ou seja se adaptaram a nova situação e/ou criaram fontes alternativas de energia. Isso não quer dizer que a infra-estrutura de energia não seja crítica, mas sim que essa infra-estrutura está mais adaptada a problemas, ou melhor dizendo, ela já foi analisada por diversas vezes, criando uma base de aprendizado enorme, na qual vários planos de melhorias já foram elaborados e executados.

Agora considerando que telecomunicações é uma infra-estrutura recente em todos os países do mundo, esse aprendizado pelo tempo (experiência) ainda não é amplamente conhecido, o que faz com que as maiorias das vulnerabilidades ainda não sejam plenamente identificadas, criando assim um setor mais frágil. Agregado a esse fato, a infra-estrutura de telecomunicações é uma das mais anárquicas, pois é formada por diferentes redes com características diversas.

Somente em meados de 1980 é que se começaram os movimentos em direção à segurança da informação e à segurança da infra-estrutura de telecomunicações para a comunidade. E isso só aconteceu porque nessa época, com o advento e disseminação da internet para a população, as infra-estruturas de telecomunicações começaram a ser utilizadas com uma maior freqüência. Nessa mesma época, os Estados começaram a disponibilizar publicamente documentos e informativos sobre essa infra-estrutura, tentando iniciar uma cultura de informação sobre a infra-estrutura, apesar de que as origens desses documentos datam de 1970. Porem, até esse momento o DoD (departamento de defesa americano) manteve em suas mãos essas informações como sendo sigilosas, por se tratarem de informações de segurança nacional, e não muito diferente disso, o mesmo aconteceu com vários outros países [2].

Com isso dá para se notar que redes e telecomunicações são cada vez mais vitais ao país, pois telecomunicações é o centro para interação de todos os outros setores [4]. Antigamente não existiam dependências tão grandes dessa infra-estrutura, mas hoje em dia, mesmo sem termos noção disso, estamos completamente dependentes de telecomunicações, pois desde a água potável consumida, até a possibilidade de termos energia elétrica para acender uma lâmpada depende da infra-estrutura de telecomunicações. No caso da água potável, hoje o seu tratamento é totalmente automatizado, com muitas trocas de informações, desde a entrada no processo, até as medições e envio de informação das análises sobre a qualidade, se está apropriada para consumo, se existe a necessidade de tratamento adicional, níveis de toxidade, etc. Já com relação à energia elétrica, além dos controles, toda a logística é feita utilizando-se a infra-estrutura de telecomunicações todas as centrais são integradas e interligadas, passam informações vitais entre elas, como a detecção de uma falha, excesso de

demanda, etc. Além disso as informações que trafegam pela infra-estrutura de telecomunicações permitem que outras centrais de geração assumam aquela região, assim diminuindo ao máximo uma paralisação no sistema, e com isso, incrementando a base de conhecimento da infra-estrutura, apontando origem de falhas, maior demanda, prováveis necessidades de manutenção, etc.

Entre outros mais, essa é a maior motivação para que o Brasil crie o seu próprio plano de segurança da infra-estrutura crítica de telecomunicações.

3. DESAFIOS

O maior desafio desse trabalho, que por um outro lado é considerada também a maior motivação, é a criação de um modelo e/ou metodologia própria para o país, que leve em consideração as características particulares do Brasil.

O modelo ideal, ou padrão para a proteção da infra-estrutura crítica de telecomunicações não existe, pelo fato de que cada país tem um foco de ação, uma cultura, uma preocupação particular. Além disso, a metodologia utilizada nunca é disponibilizada em sua total e clara amplitude, pois esses planos e metodologias estão diretamente ligados no âmbito de soberania e segurança nacional, que dificulta a sua divulgação.

Uma das etapas do trabalho é a analise do setor, que inclui, validação e definição da infra-estrutura crítica de telecomunicações. É necessário considerar na análise de setor todos os aspectos críticos da infra-estrutura, desde regulamentações e leis até aspectos financeiros, a interação com sociedade e com governos, ponto de vista sócio econômico, ou seja tudo que interage direta ou indiretamente com essa infra-estrutura.

Porém, onde é encontrado uma maior dificuldade, devido a confrontos de idéias, interpretação pessoal e de grupos, é na definição dos limites da infra-estrutura crítica de telecomunicações, pois as tecnologias evoluem cada vez mais rápido e estão cada vez mais integradas, criando uma interdependência entre elas [1]. Isso faz com que uma forma de identificar os setores críticos da infra-estrutura de telecomunicações seja necessária. É preciso saber se a telefônica fixa é de fato um setor crítico, bem como a telefonia celular, por exemplo.

As telecomunicações no Brasil e no mundo têm evoluído constantemente, resultando em muitas mudanças técnicas e principalmente de paradigmas. Essas mudanças são frutos da evolução e inovação tecnológica capazes de criar novas oportunidades de negócios, não somente para o setor, mas também para praticamente todos os setores da economia. Alguns exemplos de tecnologias de ruptura são a telefonia móvel celular, a internet, a TV digital e as redes Ad Hoc [3].

No Brasil, a evolução do setor de telecomunicações ocorreu mais fortemente a partir de meados da década de 60, como braço de execução de uma política nacional que considerava as comunicações como estratégicas para o desenvolvimento e a integração do País [5]. Nessa época, a telefonia fixa possuía um papel fundamental, e a partir da década de 90 a digitalização de linhas e sistemas foi acompanhada do surgimento de novas tecnologias e produtos de comunicação baseados em novas linguagens e protocolos. Alguns destaques foram os serviços móveis celulares e a internet, que possibilitaram a criação de diversos serviços que possuem um valor incontestável para os objetivos do governo.

Atualmente, redes de diferentes tecnologias são usadas de uma forma cada vez mais transparente, tanto pela população quanto pelo governo. Um cidadão pode não apenas se comunicar pelo telefone via uma rede de telefonia fixa, mas também pode ter acesso, usando modem ou *Asymetric Digital Subscriber Line* (ADSL), a serviços ofertados pelo governo pela internet. Pelo telefone celular, o mesmo usuário é capaz de contatar alguém que usa um telefone fixo, podendo também receber mensagens eletrônicas de representantes do governo. O e-gov ou Governo Eletrônico pode ser definido pelo uso da tecnologia para aumentar o acesso e melhorar o fornecimento de serviços do governo para cidadãos, fornecedores e servidores. Estas transações ocorrem não apenas por meio da internet, mas também por meio de telefonia móvel, televisão digital, *call centers* e outros tipos de aplicações ligadas aos computadores [6].

Essa interligação entre redes distintas (rede de telefonia fixa, rede de telefonia celular, rede de dados, internet) traz grandes benefícios para a população, para a indústria e para o governo, porém traz também como conseqüência o aumento do nível de complexidade na proteção dessa infra-estrutura.

De fato, cada tipo de rede possui suas particularidades com relação à segurança, que mudam conforme o ponto de vista em que são analisados, ou seja, o conjunto de requisitos é diferente para ângulos de visão diferentes. Essa multiplicidade de visões reforça a necessidade de se conhecer o ângulo de visão para que o conjunto de requisitos possa ser definido de uma forma mais realista. Por exemplo, elementos específicos de um determinado ambiente, como a rede de telefonia celular, possuem aspectos de segurança próprios, e que ainda podem aumentar exponencialmente com a interação com outros ambientes diferentes [3].

Mas apesar disso ainda existem várias visões e várias linhas na definição da infra-estrutura crítica de telecomunicações. Uma delas defende que a infra-estrutura das telecomunicações não deve se limitar somente a telefonia fixa, para evitar uma análise incompleta e com visão limitada, é preciso tratar com a mesma importância outras redes de telecomunicações, como a rede de telefonia móvel celular, a rede de dados fornecida por operadoras de telecomunicações e a própria internet, que possui um alcance e influência cada vez maior sobre outras redes.

Esse cenário é reforçado pelo próprio governo, no qual o seu Plano Geral de Metas para Universalização dos Serviços de telecomunicações no país, por exemplo, não contemplou apenas o atendimento aos deficientes auditivos e da fala, às camadas de baixa renda e às localidades desatendidas. O plano considerou fortemente a convergência tecnológica que, através da digitalização, possibilitou a transmissão de voz, som, vídeo, mensagem, dados e internet pela linha telefônica convencional, que transformou o acesso ao Serviço Telefônico Fixo Comutado em fator estratégico, indispensável ao desenvolvimento dos países. Inúmeros são os serviços à disposição do cidadão que tem acesso ao serviço telefônico [7].

Esta definição leva também em consideração a definição da Agência Nacional de Telecomunicações (ANATEL), de telecomunicação: "1. (Dec 97057/88) comunicação realizada por processo eletromagnético. 2. (RR) qualquer transmissão, emissão ou recepção de símbolos, sinais, texto, imagens e sons ou inteligência de qualquer natureza através de fio, de rádio, de meios ópticos ou de qualquer outro sistema eletromagnético" [7]. Assim, a Rede Nacional de Telecomunicações a ser tratada (pode conter) contem os seguintes componentes: rede de telefonia fixa, rede de telefonia móvel celular, comunicação via satélite e rede de dados.

4. METODOLOGIAS EM OUTROS PAÍSES

Cada país busca minimizar os principais riscos com base na posição estratégica e dos interesses nacionais dentro do cenário mundial. Fica claro que, atualmente, o que mais preocupa a grande maioria dos países com relação à sua infra-estrutura crítica de telecomunicações são as ações terroristas, não só pelo fato da integridade, mas principalmente pelo fato de que essa infra-estrutura pode ser utilizada para obtenção de informações importantes na comunicação entre células terroristas espalhadas pelo mundo [3].

Os estudos sobre a proteção da infra-estrutura crítica de telecomunicações estão mais avançadas em diversos outros países. Atualmente várias metodologias já estão sendo adotadas em outros países, apesar do diferente ponto focal de cada país. Todas convergem basicamente para o mesmo fim, com uma definição e criação de um modelo claro dos setores críticas, ou das infra-estruturas críticas.

Análises mostram que não existe uma metodologia melhor ou pior, simplesmente cada metodologia foi criada em particular para atender a determinado país.

Como exemplo, recentemente a Rússia começou a examinar estratégias de proteção de sua infra-estrutura de telecomunicações e informação eletrônica. O principal objetivo é desenvolver uma base para proteção da informação estratégica para o país. Para tal fim, o governo tem introduzido emendas e regulamentações para as telecomunicações. Todo o programa de proteção será desenvolvido em conjunto com o setor privado [9]. Para o Brasil essa mesma linha deve ser seguida.

A agência de inteligência russa FSB "*Federal Security Service*", sucessora da KGB, está preparando políticas e requisitos técnicos para facilitar operações em redes de computadores. SORM "*System for Ensuring Investigated Activity*" é um conjunto de regulamentações e equipamentos tecnológicos, que visam facilitar o acesso do FSB a todas as comunicações baseadas em computador,

documentos internos de operadoras de telecomunicações, incluindo telefone e internet [10]. Além disto, a Rússia, similarmente aos EUA e China, já conta com um sistema anti-satélite (ASAT) [3].

A Rússia conta também com o RU-CERT "*Russian CERT*", fundado em 1998. RU-CERT foi concebido para servir a RBNET "*Russian Backbone Network*", mas pode ser utilizado por todos usuários russos. A RBNET é uma rede que fornece conexão com a internet para comunidade científica e universidades russas. É uma espécie de RNP (Rede Nacional de Pesquisa) russa. Os principais objetivos do RU-CERT são [11]:

- Fornecer um ponto de contato confiável para tratamentos de incidentes de segurança, para usuários da RBNET;
- Responder e tratar incidentes de segurança, que ocorreram ou podem acontecer com a RBNET ou com todos os usuários de internet na Rússia, prevenção, coleta de evidências, etc;
- Fornecer consultoria e educação;
- Fornecer assistência junto às organizações legais russas, incluindo polícias;
- Fornecer assistência aos usuários russos [3].

5. CONCLUSÃO

Em um cenário onde a informação e os métodos de sua disseminação são cada vez mais estratégicos não apenas para os cidadãos, mas também para o próprio país, conhecer e analisar os pontos críticos relacionados é fundamental. Afinal de contas, a soberania nacional está em jogo, principalmente em situações que envolvem interferência política, comercial, econômica ou tecnológica de países estrangeiros.

As próprias necessidades advindas da natural evolução do papel das telecomunicações no desenvolvimento de atividades cotidianas reforçam as premissas de se aplicar os princípios constitucionais. No caso da segurança, a importância de se conhecer todos os aspectos envolvidos é ainda mais forte porque não é apenas a voz que passa pela infra-estrutura de telecomunicações, mas sim informações de toda natureza, que representam interesses nacionais que, portanto devem ser protegidas. O desafio de relacionar os interesses nacionais, a infra-estrutura de telecomunicações e os aspectos de segurança envolvidos fazem com que seja necessária uma visão ampla sobre o assunto, principalmente com relação à própria segurança, que expande até mesmo a visão da própria ANATEL.

A proteção da infra-estrutura de comunicações de um país é vital, pois todos os setores da economia, além do governo, fazem uso dos serviços de telecomunicações em seus processos de negócios. Empresas estratégicas para um país podem sofrer ataques de espionagem industrial, roubo de propriedade intelectual, etc, que representam uma séria ameaça à soberania nacional. Impactos à economia, à competitividade das empresas nacionais e ao desenvolvimento tecnológico do país também podem ocorrer [3]. Além disto, outras infra-estruturas críticas, tais como distribuição de energia elétrica e água, podem ser afetadas por ataques às redes de telecomunicações [8].

Como já discutimos, cada país criou a sua própria metodologia, pois apesar do principal objetivo (proteção da infra-estrutura crítica) ser o mesmo, as diferenças e interesses de cada País são diferentes, o que justifica a necessidade de uma contextualização

É possível observar que a preocupação dos Estados Unidos e da maioria dos países na Europa é com relação ao terrorismo. Já a preocupação principal da China é com relação à censura, enquanto a África do Sul está mais preocupada com combate à criminalidade.

Já o Brasil, com as suas particularidades e abrangência da infra-estrutura de telecomunicações, possui características próprias que direcionam a definição da metodologia para o lado da proteção de informações estratégicas.

A metodologia para a proteção da infra-estrutura crítica de telecomunicações do Brasil, leva em consideração todo os contextos envolvidos, tornando-a mais efetiva para a realidade do país.

6. REFERÊNCIAS BIBLIOGRÁFICAS

[1] Strogatz, Steven H. "Exploring Complex Networks"
[2] CIIP Handbook 2004
[3] Emilio Tissato Nakamura e Marcelo Barbosa Lima "Estratégias de Proteção da Infra-Estrutura Crítica da Informação", Aspectos Básicos do Projeto PD.30.11.69.A.023A/RT-01-AA, mar. 2004.
[4] Bruce Don, CTI – RAND
[5] Ministério da Ciência e Tecnologia. Programa Sociedade da Informação. Sociedade da Informação no Brasil - Livro Verde. Anexo 3 – Informática e Telecomunicações no Brasil. http://www.mct.gov.br/Temas/Socinfo/Livro_Verde/ca03.pdf.
[6] http://www.governoeletronico.e.gov.br/index.htm
[7] Agência Nacional de Telecomunicações, ANATEL. Análise de 27 de maio de 2003, sobre Novos condicionamentos ao Plano Geral de Metas para a Universalização do Serviço Telefônico Fixo Comutado Prestado no Regime Público – PGMU - Anexo à Consulta Pública nº 426, de 27 de dezembro de 2002. http://www.anatel.gov.br/biblioteca/analises/valente/2003/analise_av_089_2003_anexoc.pdf.
[8] The National Strategy to Secure Cyberspace. The White House. Fevereiro de 2003.
[9] "APEC TELECOMMUNICATIONS AND INFORMATION WORKING GROUP BUSINESS FACILITATION STEERING GROUP". Minutes Of Meeting. Coréia, Setembro de 2001.
[10] http://archive.aclu.org/echelonwatch/
[11] http://www.cert.ru/Eng/

O ESPAÇO CIBERNÉTICO E SEU EMPREGO COMO AGENTE DE INSTABILIDADE DE UMA NAÇÃO: UMA VISÃO SOBRE A GUERRA CIBERNÉTICA

Edson Kowask Bezerra, Emilio Tissato Nakamura,

Marcelo Barbosa Lima, Sérgio Luís Ribeiro

CPqD - Centro de Pesquisa e Desenvolvimento - Telecom & IT Solutions
Rod Campinas – Mogi-Mirim, km 118,5 – SP340 – CEP 13086-902 Campinas/SP
{kowask, nakamura, mlima, sribeiro}@cpqd.com.br

Abstract

The objective of this article is to present a definition about cyberwar. It contexts about reality current available and computer networks, confidential and authenticity of the critical infrastructure systems. Some examples of cyber war are presented and identified and some types computer networks of critical systems that can be used as possible target in cyber war creating an instability in a countries. The article presents an overview of Brazil's situation and some suggestions about implementation for improving of the information's security for our critical infrastructure

Palavras-Chaves: cyberwar, cybercrime, guerra cibernética, segurança, disponibilidade

1. INTRODUÇÃO

No processo natural de globalização que vive atualmente a humanidade, a tecnologia da informação tem tido um papel preponderante. A proximidade e facilidades por ela proporcionada têm permitido um crescimento humano e social em todos os sentidos, inclusive no aspecto de segurança e da falta desta. É comum vermos divulgados em todos os meios de comunicação falhas e problemas ocorridos tem um espaço extra aqui que tiveram como origem a não observância de algum princípio em uma das dez áreas de conhecimento da segurança em TI definidos pelo ISC2.

A descoberta de falhas e vulnerabilidades nos diversos processos que envolvem a segurança de TI tem permitido o surgimento e o crescimento do chamado *cybercrime*. Este, como uma evolução natural, tem permitido surgir uma nova linha de hipóteses de guerra chamada *cyberwar*, a guerra cibernética.

Neste artigo pretendemos iniciar uma identificação e análise da *cyberwar* e seus possíveis reflexos para a segurança nacional do Brasil, tendo como base para estudo os serviços críticos, principalmente os relacionados ao campo das Telecomunicações e Redes.

2. IDENTIFICAÇÃO CONCEITUAL

A evolução da tecnologia da informação tem permitido à humanidade um crescimento exponencial do conhecimento como nunca visto em toda sua história. A facilidade gerada pelo uso da tecnologia tem permitido a descoberta de novos benefícios e de novas áreas de estudo em todos os setores. Junto com esta explosão de conhecimentos existem àqueles que buscam achar formas de, através do uso desta mesma tecnologia, auferirem ganhos de qualquer tipo em detrimento de outros indivíduos e/ou entidades.

O *cybercrime* é aquele realizado através dos meios computacionais e com o uso de variadas tecnologias contra pessoas ou entidades com o intuito de auferir benefício próprio ou prejudicar a estrutura de funcionamento ou a imagem pública do atacado.

Em 23 de novembro de 2001, quarenta e três países, incluindo os Estados Unidos, Canadá, África do Sul, Japão e estados-membros do Conselho da Europa, assinaram em Budapeste, a Convenção Internacional contra o Cibercrime. Este tratado qualificou o cibercrime em quatro tipos: os crimes contra o sigilo, integridade e disponibilidade dos dados e sistemas; crimes digitais, como as falsificações e fraudes; as infrações relativas ao conteúdo dos dados, como os de pornografia infantil; e as infrações relacionadas à propriedade intelectual.

Numa evolução um pouco mais complexa de cybercrime, chegamos ao ciberterrorismo. Nesse tipo de crime, grupos e/ou entidades associadas a governos ou não atuam com o objetivo de disseminar o terror. Dentre os estados de gradação do medo, o terror é um dos seus estados mais intensos e aplicado por um período prolongado, visando criar uma desestabilização a partir da exploração maciça e de forma desordenada de problemas que afetam a população de modo geral. Isso causa insegurança e desconfiança na capacidade do governo de solucionar problemas, levando à instabilidade política.

O terrorismo cibernético age como a Guerra Psicológica atuando de forma dissimulada através da divulgação de notícias falsas e boatos, que se difundem rapidamente, agindo contra agentes do governo e outras entidades de renome nacional, com o objetivo de derrubar o governo. Quem atua nestes grupos são insatisfeitos com a política do governo ou simplesmente hackers que se aliam a uma determinada causa temporariamente em busca de notoriedade.

Numa posição mais elevada, temos a *cyberwar* (guerra cibernética ou ciberguerra), que tem como objetivos levar o inimigo a uma situação de paralisia estratégica. Esta é alcançada quando são atacados os centros dos poderes civil e militar e ainda os principais centros de comunicação e controle dos chamados serviços críticos, como sistemas de comunicações, saúde pública, energia e outros.

Devemos, neste ponto, destacar uma característica comum ao cibercrime, ciberterrorismo e ciberguerra: todos eles possuem em suas ações um caráter transnacional. Isso significa que, em muitas situações, não é possível identificar a origem de um ataque ou seus responsáveis, pois suas ações, vítimas e autores ultrapassam as fronteiras geopolíticas estabelecidas entre as nações, transbordando suas fronteiras físicas e dificultando a ação do direito público em virtude da dificuldade de se caracterizar as responsabilidades e responsáveis.

3. GUERRA CIBERNÉTICA

Após termos conceituados a ciberguerra, vejamos seu processo de emprego e atuação.

O conflito cibernético se caracteriza pelo uso dos meios computacionais para ações ofensivas através de penetração nas redes de computadores de alvos estratégicos cibernéticos a fim de infligir no inimigo o enfraquecimento das suas defesas convencionais, destruir a sua coesão e diminuir sua capacidade de controle, comunicações e reação ou ainda de condutas defensivas através de ações pró-ativas e reativas, visando coibir a atividade do atacante em nossa infra-estrutura de redes.

As ações ofensivas de uma guerra cibernética são iniciadas usando a infra-estrutura da internet e, de acordo com seu caráter transnacional, podem ter origem no estado inimigo ou em outros estados em que existam grupos que simpatizem com a causa do inimigo ou ainda que possuam redes que possam ser usadas como escravas (slave) num ataque. A possibilidade de participação de grupos simpatizantes ou redes escravas torna uma ação ofensiva de guerra cibernética praticamente devastadora, pois estes grupos dificultam a descoberta das origens dos participantes e tornam a adoção de medidas para neutralizar estas ações, perigosas por poderem afetar inocentes ou ainda por forçar uma conduta em um Estado que está neutro no conflito.

Estas características, no plano ofensivo da guerra cibernética, permitem ao atacante o emprego maciço de todos os recursos e meios disponibilizados com o uso das redes de computadores, bem como incentiva a criação de técnicas mais sofisticadas e a sua divulgação em sites *hackers*, produzindo uma horda de novos atacantes entre os simpatizantes da causa e entre os que buscam destaque no mundo *hacker*. Este processo de divulgação pode vir a criar um círculo vicioso que dificultará as futuras ações defensivas.

Os ataques à infra-estrutura e intrusões são extensivos o bastante para romper ou destruir a funcionalidade de grandes áreas geográficas, derrubar grandes indústrias, ou ainda, se ocorrerem diversos ataques em um padrão aparentemente coordenado, o país pode não conseguir sustentar seus negócios e seus serviços críticos. De algum modo, o país terá de possuir um plano de emergência nacional para fazer frente a estes ataques.

4. ALVOS DE GUERRA CIBERNÉTICA

Neste tipo de conflito, em que o emprego de combate entre tropas parece distante, o levantamento de informações nas redes, o roubo de arquivos confidenciais e a identificação de possíveis alvos que possam vir a permitir a conquista do poder sobre um inimigo são importantíssimos. O uso dos recursos computacionais em um ataque tem como finalidade, em uma ação de surpresa, impedir ao inimigo o uso do seu potencial de comando e controle, bem como infligir baixas em setores críticos de sua infra-estrutura nacional, não permitindo a ele uma reação e causando em sua população insegurança, desconfiança e decepção, diante de um inimigo invisível e desconhecido.

As ações numa guerra cibernética visam quebrar a disponibilidade, confidencialidade e integridade dos sistemas críticos e do poder central, causando perdas econômicas e descrédito no governo. Em relação a custos financeiros, ataques realizados em alvos comerciais trazem um maior prejuízo financeiro, causado pela perda do lucro no período em que este fica fora do ar, muito maior do que o realizado em alvos do governo. Entretanto, os ataques realizados sobre sites governamentais trazem um maior peso sobre o moral, pois causam humilhação pela incapacidade de manter ativo um site ou uma atividade do próprio governo.

É óbvio que todos os setores da infra-estrutura nacional dependem das telecomunicações para a operação eficiente – algumas vezes, para todas as operações – e, também é sabido que o presente nível de dependência da tecnologia de informação e sistemas baseados em computadores representam, para alguns aspectos da infra-estrutura dos serviços críticos, a base da informação para que possam também funcionar. Da mesma forma, a energia elétrica é absolutamente essencial para as facilidades e funções dos equipamentos, mantendo o padrão mínimo das operações.

Partindo dessas premissas, já podemos inferir como alvos vantajosos para uma guerra cibernética, segundo a importância das suas infra-estruturas, as redes de computadores e sistemas que gerenciam e controlam os serviços críticos de:

a) Redes de Telecomunicações
b) Energia Elétrica
c) Saúde Pública, Emergência e Água potável
d) Sistema Financeiro
e) Redes de Comando e Governo

As redes dos sistemas de telecomunicações formam a estrutura básica das comunicações e informações e, com ela desativada, perde-se o meio de transmissão de notícias, decisões e informações. Sua ruptura deixa os responsáveis em todos os níveis de governo e da sociedade civil sem contato, e pode gerar, no seio da sociedade, uma incerteza com relação à situação em virtude dos boatos e dúvidas que passam a existir pela falta de informações.

As atuações sobre os sistemas de energia elétrica visam reduzir e dificultar a capacidade de recuperação de um ataque sobre os sistemas de telecomunicações e também trazer a insegurança pelas ocorrências de diversos blecautes.

Os serviços prestados pelas redes de Saúde Pública, Emergência e sistemas de distribuição de Água Potável são essenciais para a população de modo geral. Quando estes serviços críticos ficam indisponíveis em virtude de um ataque cibernético, deixam a população sem os apoios que considera básicos, além de trazerem a desconfiança pela qualidade dos serviços de água, gerando insegurança e medo. Os três serviços são colocados no mesmo nível, pois todos afetam o bem-estar sanitário da população. Este tipo de ataque abre caminho para que a própria população se insurja contra o governo pela sua falta de capacidade de prestar estes serviços.

Já sobre o sistema financeiro, principalmente sobre o banco central e as redes dos grandes bancos e corretoras, visa causar uma quebra na estrutura econômica do país, levando ao caos financeiro nacional, que poderá ter reflexos na solidez deste país na economia internacional.

Um ataque cibernético sobre as redes de governo e de comando central tem como objetivo reduzir ou tirar a capacidade de chefia e liderança tanto do governo como de seus principais centros de comandos militares. Esta ação vai reduzir drasticamente a capacidade de recuperação e respostas aos ataques cibernéticos.

Estes são apenas os cinco alvos que consideramos mais críticos. Podemos e devemos, numa análise visando construir um Plano Nacional de Segurança das Informações, identificar outros sistemas que são críticos ao país e à população, tais como sistemas de distribuição de combustíveis, sistemas aeroportuários, sistemas do judiciário, sistemas dos programas assistenciais, etc.

5. GUERRA CIBERNÉTICA NO MUNDO

Até aqui, temos a impressão de que falamos de algo que nos parece fora da realidade. Porém temos exemplos de que uma guerra cibernética está muito mais próxima da realidade do que possamos imaginar.

Vejamos alguns exemplos:

5.1. Estados Unidos da América (EUA) x China

A China é hoje um dos maiores produtores de vírus e um dos países que possuem uma doutrina de guerra cibernética. O livro "Guerra Irrestrita", dos coronéis Qiao Liang e Wang Xiangsi, propõe uma "guerra assimétrica", que não possui regras, e que prega, entre outros, que devem ser atacadas as redes de computadores americanas.

Em 1999, um bombardeio dos EUA à embaixada da China em Belgrado provocou um processo de retaliação de hackers chineses que atacaram sites do governo americano e invadiram diversos outros sistemas numa ação coordenada e com objetivos definidos.

Em 2001, quando um avião americano se chocou em pleno ar com um avião chinês ocasionando a morte do piloto chinês e a prisão da tripulação americana também houve um ataque cibernético. Como forma de retaliação, *hackers* chineses atacam sites do governo americano e descobrem a existência de uma rede de testes de transmissão de energia elétrica desprotegida na Califórnia.

A China é um país que vem se destacando na formação de hackers com o objetivo de usá-los como combatentes cibernéticos, no caso de uma necessidade.

5.2. Israel x Autoridade Nacional Palestina

Em setembro de 2000, jovens hackers israelenses interferem nos sites do Hezbollah e do Hamas no Líbano. Com ataques constantes, bloquearam os serviços em seis sites destas organizações no Líbano e da Autoridade Nacional Palestina. Este ataque gerou uma guerra cibernética. Palestinos e organizações islâmicas clamaram por uma Guerra Santa Cibernética.

Em pouco tempo, os hackers pró-Palestina atacaram os sites do parlamento, o ministério do exterior e a força de defesa de Israel. Em seguida atacaram o gabinete do primeiro-ministro, o Banco de Israel e a bolsa de valores. Sites foram desfigurados, causando prejuízos a programas sociais israelenses aos idosos e houve tentativas de tirar do ar os principais serviços de ISP de Israel.

Estudos feitos posteriormente estimam que havia apenas trinta hackers principais envolvidos no conflito cibernético palestino-israelense.

5.3. Outros exemplos

James Adams cita, em seu livro "The Next World War", que, em 1997, os Estados Unidos organizaram um exercício simulando uma crise internacional com um governo estrangeiro que havia contratado trinta e cinco hackers para neutralizarem as ações dos Estados Unidos.

Com material adquirido no comércio, os hackers foram bem sucedidos na simulação, demonstrando que podiam chegar facilmente às malhas energéticas de todas as principais cidades americanas e conseguiram penetrar no sistema de emergência 911. Poderiam facilmente ter tirado as duas redes do ar. Após isso, acessaram o sistema de comando do Pentágono e verificaram 40.000 redes, obtendo acesso a trinta e seis delas.

Isso demonstra a facilidade com que apenas trinta e cinco hackers conseguem entrar em sistemas desprotegidos ou fracamente protegidos e impedir que os Estados Unidos respondessem a uma crise.

5.4. Situação do Brasil

Atualmente no Brasil, não existe concretamente uma política de segurança das informações que se preocupe com este estado da arte que é a guerra cibernética. Não é um assunto apenas de governo e forças armadas, mas sim um projeto que envolve todos os setores da sociedade, pois todos são e estão dependentes da infra-estrutura das redes de computadores.

Em muitos países, esta preocupação já está inserida nas políticas de governo, em virtude das suas conseqüências prejudicarem toda a nação. Para a criação destas políticas de segurança, é preciso a criação de uma mentalidade de segurança em todos os níveis da sociedade civil. A partir daí, devem-se levantar as vulnerabilidades existentes na infra-estrutura dos serviços críticos.

Até agora, o Brasil tomou poucas iniciativas de identificar quais seriam nossos serviços críticos, suas vulnerabilidades e as medidas que permitem a redução ou a eliminação dessas vulnerabilidades. Este é um trabalho permanente e que deve contar com a participação do governo e empresas.

Entretanto não podemos deixar de reconhecer a importância de alguns passos que já foram dados. O primeiro foi a criação do Comitê Gestor da Segurança da Informação (CGSI) em 2000 e, a partir de um trabalho deste CGSI, houve a criação de diversos Grupos de Trabalho (GT) no decorrer de 2003, dentre os quais merecem destaque o Grupo de Trabalho do Centro de Emergência de Computação e o Grupo de Trabalho de Política Nacional de Telecomunicações. É uma iniciativa bastante louvável, mas que tem que ter continuidade e deve gerar medidas preventivas a serem implementadas por todos os setores envolvidos em infra-estrutura dos serviços críticos.

6. PERSPECTIVAS FUTURAS DE GUERRA CIBERNÉTICA

À primeira vista, parece um estudo alarmante, mas não podemos deixar de acreditar que as armas para iniciar esta guerra estão nas mãos de cada usuário de computador.

O uso de computador como uma ferramenta de ação criminosa, o cibercrime, já é um fato do nosso cotidiano. E o uso deste mesmo computador como ferramenta também de ações de guerra é uma perspectiva que não pode deixar de ser analisada por nenhum país.

Nessa guerra cibernética, o *hacker* como ferramenta de combate passa a ocupar uma posição fundamental que já foi ocupada por outros combatentes. Cabe aqui uma análise da importância da formação desse guerreiro cibernético, que vai ter a responsabilidade de infligir baixas sem causar diretamente as mortes tão comuns nos outros tipos de guerras.

Nesse tipo de conflito, a preocupação com a segurança das informações passa a ser essencial para fornecer capacidade de lutar, mas também para fornecer a capacidade de se preparar e reagir diante de um possível ataque. O estudo para o entendimento da segurança das informações a fim de capacitar para levantamento de vulnerabilidades e riscos dos diversos e variados sistemas de redes deve ser estendido aos nossos cursos de graduação a fim de permitir a formação da mentalidade de segurança da informação. Teremos que nos preocupar com a proteção dos nossos sistemas e também com a formação do material humano para o gerenciamento da segurança da informação sob todos os aspectos.

A garantia da disponibilidade, confidencialidade e autenticidade deve ser um objetivo constante, pois é exatamente em cima desses fatores que são realizados os ataques cibernéticos. Quebrada a disponibilidade de um sistema de redes de um serviço crítico, os prejuízos são enormes e, a partir daí, derruba-se a confidencialidade e a autenticidade, gera-se o caos e cria-se a instabilidade, que poderá, em pouco tempo, causar a paralisia estratégica.

7. CONCLUSÃO

O espaço cibernético possui hoje milhões de usuários numa escalada de crescimento vertiginoso a cada minuto. São pessoas ligadas à internet através das mais variadas estruturas de redes e, na maioria delas, sem qualquer política de segurança e num regime anárquico, onde não existe um mínimo controle. Esta falta de políticas, processos e controles, facilitam a disseminação de atividades criminosas no espaço cibernético.

A preocupação com a disponibilidade, confidencialidade e autenticidade não deve estar restrita apenas às empresas, mas também aos governos onde esta preocupação deve estar incorporada às Políticas de Segurança de Informação Nacional. Estas devem ser escritas baseadas em contínuos levantamentos de vulnerabilidades e análises de risco, buscando sempre máxima resiliência.

Como padrão no combate ao crime, a proteção contra os crimes de computadores começam pela prevenção. A criação de centros de pesquisa e estudo da segurança das informações é um passo grande em direção à criação de metodologias e disseminação da cultura de segurança computacional. As grandes empresas e os governos precisam treinar grupos de análise de risco, gerência de crises, identificando as ameaças ao sistema, as suas vulnerabilidades e as contramedidas a serem adotadas, bem como coletar todos os indícios e provas, colaborando assim com uma eventual investigação.

A criação de uma metodologia para identificação de vulnerabilidades e riscos de âmbito nacional é um caminho natural que deve conduzir ao levantamento das infra-estruturas de serviços críticos diante de uma possível guerra cibernética. A palavra de ordem é se preparar adquirindo conhecimento, antecipar com o levantamento e análise, e agir o mais rápido possível como a Era Digital exige.

8. *REFERÊNCIAS BIBLIOGRÁFICAS:*

Sampaio, Fernando G., Ciberguerra, Guerra Eletrônica e Informacional, 26 de abril de 2001.

Michelle Delio, "It's (Cyber) War: China vs U.S." disponível no endereço www.wirednews.com/news/print/0,1294,43437,00.html, 30 de abril de 2001.

Allen, Patrick e Demchak, Chris, "A guerra cibernética entre Palestina e Israel", MilitaryReview, edição 1º trimestre de 2003.

Adams, James, "The Next World War", Ed Simon & Schuster, 23 de março de 2001.

Liang, Qiao e Xiangsi, Wang "Unrestricted Warfare"

Vários, "In Athena's Camp: Preparing for Conflict in the Information Age", 2002

International Information Systems Security Certification Consortium, Inc, no endereço www.isc2.org

CONCEITOS E PROCEDIMENTOS EM ANÁLISE DINÂMICA DE CÓDIGO BASEADO EM SISTEMAS WINDOWS

Adriano Mauro Cansian, Thiago Alves Siqueira, César Eduardo Atílio

UNESP – Universidade Estadual Paulista
{adriano,thiago}@acmesecurity.org

Resumo

A Internet atualmente está sendo usada para a prática de crimes eletrônicos. Com isso, cresce a necessidade de que técnicas de perícia forense sejam utilizadas para coleta de evidências digitais,que possam ser usadas para apurar quem são os meliantes e gerar uma contra-medida contra cada tipo de ataque. Diante deste cenário, este artigo irá mostrar vários conceitos, técnicas e metodologias pertinentes à disciplina de perícia forense computacional, mais especificamente aà análise dinâmica de código em ambientes Windows. Ao final, será feito um estudo de caso de um código malicioso que circulou na internet brasileira no início de 2003.

1. INTRODUÇÃO

Atualmente, a Internet é utilizada para os mais diversos fins. Informações confidenciais e valiosas trafegam pela rede. Este tipo de informação é um atrativo para meliantes, que, em posse delas, pode tirar proveito da vítima e trazer benefícios a si, sendo isso um crime. Dessa forma, técnicas de perícia forense computacional devem ser utilizadas para obtenção de informações de como isso ocorreu. Diante desta situação, este trabalho irá descrever conceitos e metodologias de perícia forense computacional, mais especificamente da análise dinâmica de código, voltadas ao sistema operacional Windows. Ao final, será feito um estudo de caso de um código malicioso que circulou na Internet brasileira no início de 2003.

2. CIÊNCIA FORENSE COMPUTACIONAL

Para o escopo deste trabalho,é considerado e entendido que a Ciência Forense Digital consiste no uso de métodos científicos na preservação,coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidência digital. Seu propósito é facilitar ou possibilitar posterior reconstrução de eventos criminais[1]. Para suportar os resultados de uma análise forense são necessários procedimentos e protocolos detalhados, documentados e revisados, aceitos pela comunidade científica relevante[2].Para tal,a seguir,serão apresentados os procedimentos para uma análise dinâmica de uma evidência digital.

2.1. Análise de programa

Uma das maneiras, entre as várias existentes, para análise de programa, é o estudo dinâmico do artefato. Sua vantagem em relação a outros métodos é que ela pode ser rápida e precisa. Sua desvantagem é que a saída da análise obtida é tudo que se possui como resultado.

2.2. Análise dinâmica

O primeiro conceito a ser definido é o de código malicioso (artefato). No contexto em que estamos trabalhando, código malicioso é um termo geral que se refere a programas projetados para efetuar algum tipo de atividade não autorizada em sistemas computacionais. A análise dinâmica de artefatos é um processo minucioso, baseado na execução do código malicioso, observação e monitoração de todas as alterações causadas no sistema em tempo real. Os passos para a realização de uma análise serão explicitados ao longo do artigo.

3. METODOLOGIA DE ANÁLISE

3.1. Máquina que será usada na análise

Um ambiente confiável deve ser preparado para a utilização no processo de análise. Deve-se levar em conta o equipamento e sistema operacional alvo do artefato e o que se deseja adquirir com a análise.

O ambiente de análise deve ser isolado de uma rede de produção,para que se evite possíveis ataques a esta.Isso pode ser feito por filtros de contenção de tráfego.

Determinado que um programa deve ser analisado é necessário coletá-lo e gerar um *hash* criptográfico[4]. Esta é uma técnica importante, pois atribui unicidade ao artefato. Assim, pode-se compará-lo com outros artefatos, e, caso esse *hash* seja semelhante, já se sabe que o código malicioso é o mesmo. Havendo alguma análise pronta, não é necessário uma nova, o que pode se determinar pelo *hash*.

3.2. Preparação do ambiente

O ambiente de análise deve possuir o equipamento e o sistema operacional alvo do artefato. Deve-se utilizar um ambiente exclusivo para análise, afinal, após a mesma, estará impróprio para utilização como ambiente de produção. Este ambiente deve possuir todos os serviços requisitados pelo artefato. Dessa forma pode-se obter total performance do código, podendo cobrir todos os fluxos possíveis em seu código fonte.

Quaisquer alterações realizadas no sistema não devem passar desapercebidas, e, para isso, deve-se utilizar as ferramentas corretas. Dependendo do sistema operacional, comportamentos diferentes são esperados. No sistema operacional Windows, por exemplo,espera-se que o registro do sistema seja alterado. Deve-se, então, monitorá-lo.

Além das alterações locais, podem ocorrer alterações remotamente. Inúmeros artefatos têm como objetivo disparar ataques remotos contra outros computadores. Deve-se, portanto, permitir que haja conexões externas, mas de forma controlada. Para isso, pode-se usar filtros no *firewall* [5] desta rede para bloqueá-las. Outra forma é uma rede isolada com os serviços requisitados.

Um analista de artefatos deve conhecer o maior número de ferramentas para análise para o maior número de sistemas operacionais possíveis, de maneira a ser eficiente e eficaz. Isto porque a análise dinâmica é um processo onde deve-se definir rapidamente as conseqüências causadas pelo artefato e as contra-medidas.

3.3. Evidências digitais

O termo evidência digital refere-se a toda e qualquer informação digital capaz de determinar que um incidente ocorreu.

Dan Farmer e Wietse Venema introduziram um conceito denominado de ordem de volatilidade [6], que diz que o tempo de vida de uma evidência digital varia de acordo com o local onde ela está armazenada. O detalhamento de cada fonte de informação e das técnicas utilizadas para sua extração é apresentado a seguir.

3.4. Coleta de evidências

A busca de evidências em um sistema computacional constitui-se de uma varredura minuciosa nas informações que nele residem, sejam dados em arquivos ou em memória, "deletados" ou não, cifrados ou possivelmente danificados [7].

Em uma investigação do comportamento de um programa, deve-se obter informações sobre o estado corrente do sistema. O estado da máquina comprometida não pode ser alterado. Assim, as informações devem ser gravadas em outra máquina ou a saída das ferramentas de coleta de informações direcionadas para a máquina forense. Para isso, uma boa ferramenta é o *netcat*[1].

Na máquina forense que está recebendo o redirecionamento dos comandos, pode-se utilizar ferramentas diretamente de um CD-ROM. Garante-se dessa maneira que as ferramentas utilizadas para a análise não serão modificadas pelo artefato.

4. COLETANDO INFORMAÇÃO VOLÁTIL

4.1. Processos

Informação volátil pode ser descrita como a informação que representa o estado corrente do sistema. O primeiro item de interesse de um investigador é o conjunto de processos em execução no sistema, pois tais informações podem revelar evidências de atividades não autorizadas. Esse tipo de informação pode ser obtida pelo *Pslist.exe*[2], que provê uma lista dos processos em execução, o número de identificação do processo (PID), e a quantidade de tempo de início de execução, além dos dados sobre a carga de processamento. *Fport.exe*[3] age do mesmo modo, fornecendo além daquelas informações o caminho do comando executado e as portas TCP e UDP abertas referentes ao processo. *Listdlls.exe*[4] lista as DLL's[5] que estão em uso em cada processo e o caminho das DLL's carregadas.

4.2. Conexões de rede

O estudo das conexões de rede provê informações valiosas acerca das conexões em andamento e dos processos aguardando uma conexão [8]. Assim, é possível determinar se existe alguma conexão não autorizada em andamento. Isto pode ser feito utilizando as ferramentas *netstat*[6] e *nbtstat*[7].

Uma outra informação volátil consiste no tráfego enviado pelo sistema comprometido a outros hosts. Exitem vários programas para Windows que utilizam as bibliotecas *winpcap*[8], comumente denominados de *sniffers*. O exemplo mais comum desse programas é o *Ethereal*[9].

---

[1] O programa netcat e maiores detalhes sobre o mesmo podem ser encontrados na URL http://www.atstake.com/research/tools/network_utilities/ (disponível em Maio de 2004).

[2] O programa pslist.exe e informações adicionais sobre o mesmo podem ser encontradas em http://www.sysinternals.com/ntw2k/freeware/pslist.shtml (disponível em Maio de 2004).

[3] O programa Fport.exe e informações adicionais sobre o mesmo podem ser encontradas em http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/overview.htm (disponível em Maio de 2004).

[4] O programa Listdlls.exe e informações adicionais podem ser encontradas em http://www.sysinternals.com/ntw2k/freeware/listdlls.shtml (disponível em Maio de 2004).

[5] Maiores informações sobre DLL em http://support.microsoft.com/default.aspx?scid=kb;en-us;815065 (disponível em Maio de 2004).

[6] O programa Netcat e informações adicionais podem ser encontrados em http://www.atstake.com/research/tools/network_utilities/ (disponível em Maio de 2004).

[7] Maiores informações sobre o nbtstat podem ser encontradas em http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/nbtstat.mspx (disponível em Maio de 2004).

[8] Maiores informações sobre o Winpcap podem ser obtidas em http://winpcap.polito.it/ (disponível em Maio de 2004).

[9] A ferramenta Ethereal e maiores informações podem ser obtidas em http://www.ethereal.com/ (disponível em Maio de 2004).

5. INFORMAÇÃO NÃO VOLÁTIL

Informação não volátil consiste das configurações do sistema que não mudam todo tempo, ou quando o sistema é reinicializado.

5.1. Arquivos

A fonte de informação onde o processo de análise forense geralmente mais se concentra é o sistema de arquivos. Uma das informações referentes aos arquivos que o investigador deve coletar são as marcas de tempo. Tais marcas correspondem aos tempos de última modificação no arquivo, último acesso e última mudança nas propriedades do arquivo (*MAC times*) [10]. Um exemplo de ferramenta que pode ser usado para este fim é a *afind.exe* [10].

5.2. Registro

O registro do sistema é definido como uma base de dados hierárquica usada no Microsoft Windows 9x, CE, NT e 2000 para armazenar informação necessária para configurar o sistema, aplicações e dispositivos de *hardware*. Esta base de dados pode conter evidências valiosas acerca do comportamento do código malicioso. Uma ferramenta nativa do sistema para coletar informação das entradas do registro é *Regedt32.exe* para Windows NT e o *Regedit.exe* para demais versões do Windows.

5.3. Documentação

A documentação é um processo que ocorre paralelamente ao processo de análise. Todos os passos percorridos para execução da mesma deve ser minuciosamente relatado. Nisto, envolve a descrição das ferramentas utilizadas, modo de preparação do ambiente e razão pela qual o ambiente foi montado de tal maneira. Informações obtidas pela saída das ferramentas devem ser anexadas ao documento.

Além destes dados, deve-se ter a identificação do responsável pela análise, data da coleta do artefato, *hash* criptográfico do arquivo, forma como foi coletado o artefato (e-mail, honeypot etc) e razão pela qual foi considerado um artefato.

Como conclusão, a documentação deve possuir uma maneira para solucionar o problema causado pelo artefato analisado.

6. ESTUDO DE CASO

Abaixo, é apresentado um estudo de caso consistindo em uma análise dinâmica do código malicioso *certificado_digital.exe*. Este programa foi distribuído através de correio eletrônico na Internet brasileira, em meados de maio de 2003. Trata-se de uma mensagem persuasiva de caráter cognitivo e um programa anexado. Este programa instala o artefato real MSNBC32.EXE no sistema onde foi executado.

6.1. Análise Dinâmica do artefato de risco

Análise: 12/2003
certificado_digital.exe
Sistemas Afetados: Sistemas utilizando Microsoft Windows
Codinome: falso-verisign
Hash: 7e5776f9c965307d8033433cbdbc6bde
Tamanho do Arquivo: 334567 bytes
Dados do analista: xxxx

[10] O pacote que contém o Afind e maiores informações podem ser obtidos em http://www.foundstone.com/ (disponível em Maio de 2004)

Dados do responsável pela análise: xxxx
Data e horário da análise: 13/05/2003 – 22:00 h.

6.2. *Motivações para análise*

E-mail malicioso recebido por várias pessoas com informação aparentemente não autêntica;
Tal atitude não condiz com o comportamento da empresa em questão ao enviar e-mails não solicitados;
Um arquivo acompanhado de uma mensagem persuasiva, de origem não comprovada;
Mensagens de listas de discussão relatando o comportamento parcial do artefato;
Mensagem cognitiva com erros graves de português;
Não se distribui certificados digitais por e-mail.

6.3. Ambiente de análise

Máquina Forense: Sistema operacional: Windows 98 SE
Processador: AMD Athlon 800MHZ
Memória RAM: 128MB
Disco: 2 GB
Esta máquina é integrante de uma rede que possui mais 2 máquinas utilizando o sistema operacional Linux. Esta rede é limitada por um *firewall* (Zwicky e Cooper, 2000) utilizando IPTABLES (Stephens, 2002). O objetivo destas máquinas é monitorar e capturar a interação da máquina forense com o ambiente, quando o programa for executado. Estrategicamente, o filtro de contenção tem como principal objetivo conter qualquer tipo de tráfego malicioso destinado a algum computador externo do ambiente forense.

6.4. Execução do artefato

21:54:14 O programa é executado na máquina forense descrita acima.
A saída do programa pslist.exe forneceu a seguinte informação:
Name (MSNBC32), Pid (1700), Elapsed Time (0:00:12.031)
Arquivos criados ou modificados a partir da execução do artefato:
C:\WINDOWS\MSNBC32.EXE
C:\WINDOWS\Debug32
C:\faxsetup32.txt
C:\WINDOWS\Debug32\Clickxxx.jpg
C:\WINDOWS\SERVONE32.DLL
C:\WINDOWS\SERVTW032.DLL
C:\WINDOWS\ZIPDLL.DLL
C:\WINDOWS\SYSTEM.CB (Arquivo que contém informações a respeito do teclado).
Foi notificada a criação ou modificação destes arquivos de acordo com os atributos de tempo dos mesmos, conferindo com o horário de execução do programa. Esta verificação foi realizada inúmeras vezes para garantir que as mudanças possam ser atribuídas a execução do artefato.
Alterações no registro são realizadas para que o artefato execute automaticamente quando o sistema for reiniciado. Para isso, é adicionado um novo valor de *string* no registro com o nome MSNDC32.EXE, referenciando C:\WINDOWS\MSNBC32.EXE em MyComputer\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
Quando o programa é inicializado automaticamente pelo Windows, o arquivo C:\faxsetup32.txt é criado. Outras possíveis localizações de MSNBC32.EXE no registro é RunServices, Run-, RunServices-, RunOnce.

6.5. Funcionamento do artefato

Ao iniciar sua execução, o arquivo MSNBC32.EXE cria o arquivo C:\faxsetup32.txt, que irá armazenar um sumário com a especificação do sistema, os pressionamentos de teclas bem como os

títulos das janelas de aplicativos ativas. Além disto ele correlaciona temporalmente os pressionamentos de teclas com fotos da região clicada com o *mouse*.

Os arquivos Clickxxx.jpg, gerados em C:\WINDOWS\Debug32, armazenam imagens de 25 x 25 pixels em 16 milhões de cores ao redor do cursor, quando o botão esquerdo do mouse é pressionado.

O programa captura imagens e o comportamento do sistema por aproximadamente 400 segundos. Após isso, o programa envia via correio eletrônico os arquivos faxsetup32.txt e todos Clickxxx.jpg, tendo como remetente zzz@zzz.zzz e destinatários xxx@xxx.xxx.xx e yy@yyy.yyy.yy. Segue abaixo o arquivo faxsetup32.txt gerado (Dados sanitizados):

Dados do Equipamento para Identificação

Sistema Operacional : Windows 95/98/Me
Nome do Computador : VWwin98
Versão do Sistema : xxx
Compilação do Sistema : xxxxxxxx
Sistema de Arquivo : FAT32
Nome do Disco Local : Disco Local
Serial do HD : xxxxxxxx
Data do Sistema : 5/13/03
Hora do Sistema : 10:07:55 PM
IP do Computador Local : 192.168.0.98

Janela Ativa - Servant Salamander
< Click1 >
< Click2 >
< Click3 >
<Tab> <Down> <F3> <Esc> <Down>
Janela Ativa - C:\WINDOWS\Debug32\Click2.jpg (25 x 25 x 16777216 colors - 100%) - PictView
Janela Ativa - Servant Salamander
<Esc> <Ctrl> <Alt>
< Click4 >
Janela Ativa - Microsoft Internet Explorer
< Click5 >
Janela Ativa - C:\WINDOWS\Debug32\Click9.jpg - Microsoft Internet Explorer

6.6. Comportamento anômalo do sistema obtido através da execução do artefato

Sistema apresenta perda de desempenho;
Falta de recursos ou de memória RAM;
Cursor do mouse pisca intermitentemente.

6.7. Recomendações para limpeza de máquinas comprometidas

Os seguintes passos devem ser seguidos para limpeza de máquinas comprometidas:
Se a máquina puder ser formatada:
Desconectar a máquina comprometida de rede;
Fazer cópia de segurança de arquivos pessoais;
Formatar a máquina comprometida;
Trocar todas as senhas que foram inseridas no sistema a partir do instante em que o artefato foi executado, incluindo senhas e números de cartões de crédito;

Outra opção é excluir as entradas adicionadas pelo artefato no registro e os arquivos por ele criados, citados na análise. É altamente recomendável reinstalar o sistema, modificando algumas de suas características, como por exemplo a versão do sistema operacional, o nome da máquina e o endereço IP da mesma na rede.

6.8. Conclusão da análise

Frente a este comportamento, presumiu-se que um dos objetivos do programa é capturar senhas ou informações pessoais inseridas através de uma interface do tipo teclado virtual, muito usado atualmente em sistemas *Netbanking*, e também de informações digitadas a partir do teclado. Os teclados virtuais nada mais são do que uma interface gráfica que permite a simulação do pressionamento de teclas, através do uso de cliques do mouse.

7. CONCLUSÃO

O estudo apresentado neste trabalho representa um esforço no sentido de suprir a necessidade de um melhor entendimento de como se obter e utilizar evidências eletrônicas armazenadas em computadores. A discussão acerca dos vários procedimentos envolvidos em uma análise dinâmica, detalhando metodicamente cada etapa de uma análise, fornece um guia prático para aqueles que estão iniciando na área forense computacional.

8. REFERÊNCIAS

[1] G. Palmer, "A Road Map for Digital Forensic Research," Digital Forensic Research Workshop (Dfrws), *Report* 2001.
[2] M. Noblett, M. Pollitt, L. Presley, "Recovering and Examining Computer Forensic Evidence," Forensic Science Communications, Number 4, Volume 2, U.S. Department of Justice, FBI.
[3] W. Venema, "Finding the purpose of an unknown program," Strangers In the Night, Dr. Dobb's Journal, 2000.
[4] B. Scheneier, "*Applied Cryptography",* John Wiley & Sons, New York, 1996.
[5] J. C. Stephens, "Iptables". Disponível: http://www.sns.ias.edu/~jns/security/iptables/index.html
[6] D. Farmer, W. Venema,"Computer forensics analysis class handouts". Disponível: http://www.fish.com/forensics/class.html
[7] M. Abdalla, P. Geus, "Forense Computacional: Procedimentos e Padrões", Simpósio de Segurança da Informação, 2001, São José dos Campos, Anais SSI2001.
[8] W. G. Kruse II, J. G. Heiser. "Computer Forensics: Incident Response Essentials", Addison-Wesley, Reading, Massachussetts, 2002.
[9] A. Silberschatz, P.. Galvin, "Operating System Concepts", John Wiley & Sons, New York, 5 Edição.
[10] E. Casey, "Handbook of Computer Crime Investigation", Academic Press, San Diego, Califórnia, 2000.

SEGURANÇA DO ESPAÇO CIBERNÉTICO NO CONTEXTO DE UM PAÍS

Edson Kowask Bezerra, Emilio Tissato Nakamura,

Marcelo Barbosa Lima, Sérgio Luís Ribeiro

CPQD - Centro de Pesquisa e Desenvolvimento - Telecom & IT Solutions
Rod Campinas – Mogi-Mirim, km 118,5 – CEP 13086-902 – Campinas/SP
{kowask, nakamura, mlima, sribeiro}@cpqd.com.br

Abstract

This article discusses cybersecurity in a context of a country. Protecting critical telecommunication infrastructure requires an abroad vision about different objectives and different aspects related to threats, vulnerabilities and risks, which have to be known. Some countries focuses their security initiatives on terrorism, while others focuses on industrial espionage. The necessity of securing a telecommunication infrastructure and the actions taken in some countries are evaluated, and Brazilian telecommunication sector is analyzed in an international context.

Palavras-Chaves: proteção da infra-estrutura crítica de telecomunicações, disponibilidade, segurança em telecomunicações, contexto internacional, segurança do espaço cibernético em um país

1. INTRODUÇÃO

A segurança cibernética é uma necessidade cada vez maior para cada cidadão, mas ela pode atingir proporções ainda maiores, com muitas ameaças que podem afetar todo um país. Assim como a evolução do espaço cibernético criou possibilidades para o aparecimento de novas formas de crimes contra indivíduos e empresas (tais como invasões a sistemas, roubo de informações, fraudes eletrônicas, *phishing scam*), os países também se tornam potenciais alvos de diversos tipos de ataques.

No contexto de proteção de um país, as ameaças e as vulnerabilidades envolvidas são diferentes das relacionadas com indivíduos, já que a soberania nacional é que deve ser mantida. Desta forma, a estratégia para tratar a segurança cibernética no âmbito de um país exige esforços que incluem, além da abordagem tradicional do gerenciamento de riscos, a identificação de infra-estruturas críticas a serem protegidas.

Muitos esforços estão sendo gastos em diversos países para a proteção da infra-estrutura crítica de informação. Cada um desses países define estratégias que são baseadas em um contexto específico. Os Estados Unidos, por exemplo, trata a questão da segurança do espaço cibernético com um foco especial em guerra cibernética e terrorismo. Já Portugal, além de se considerar os fatores principais de outros países, como a guerra cibernética e o terrorismo, considera também a preocupação com a espionagem como um fator de desestabilização do país, tendo assim medidas definidas para a sua prevenção e inibição.

Este artigo trata da contextualização do Brasil nesse cenário internacional de proteção de infra-estrutura crítica, com enfoque à infra-estrutura crítica de telecomunicações.

2. MOTIVAÇÃO

A segurança do espaço cibernético é um assunto que vem ganhando importância cada vez maior, fruto da constante evolução tecnológica e da maior integração entre diferentes redes, que criam muitas

oportunidades – tanto para novos negócios e serviços, quanto para novas modalidades de crimes. Isso faz com que as conseqüências e as influências resultantes dessas novas oportunidades (benéficas e maléficas) tenham que ser conhecidas e bem analisadas, para que a sociedade e o país possam aproveitar todo o potencial existente, sem que danos sejam causados.

No caso da segurança do espaço cibernético, as vulnerabilidades em infra-estruturas críticas tendem a crescer devido ao aumento da interdependência entre elas, que é cada vez mais complexa, principalmente com relação às telecomunicações. Dessa forma, uma infra-estrutura crítica (como distribuição de água, saúde pública, transportes, energia) pode sofrer influências e danos caso uma vulnerabilidade em uma outra infra-estrutura crítica, como a de telecomunicações, seja explorada.

De fato, a disseminação e integração das redes de telecomunicações fazem com que os riscos de uma interrupção, por exemplo, se difundam de uma rede para outra. Além disso, novas formas de crimes e de formas de intimidação, que podem estar relacionados a fins econômicos, sociais, políticos e até mesmo militares, fazem com que as ameaças aumentem. Isso pode ser reforçado pelo fato de ataques poderem ser realizados de uma forma anônima a uma distância segura, ou seja, são difíceis de serem detectados e responsabilizados. Outra conseqüência da disseminação das redes de telecomunicações é o aumento da dificuldade no entendimento e no controle das mesmas.

A necessidade de um país tratar da segurança cibernética sob o contexto que vai além da proteção do cidadão, assim, torna-se cada vez mais evidente. Nos casos mais extremos, quando as redes têm problemas ou não funcionam, riscos para a vida, para a liberdade e para a propriedade são causados. Isso porque a interrupção de serviços (resultantes de incidentes em diferentes infra-estruturas críticas) pode ameaçar vidas e propriedades, além de destruir ou modificar inadequadamente informações, com possíveis impactos que interrompem o trabalho de governos e corporações.

3. PROTEÇÃO DA INFRA-ESTRUTURA CRÍTICA DE TELECOMUNICAÇÕES

Em um mundo no qual a interdependência entre diferentes infra-estruturas críticas é cada vez maior, a preocupação com a sua proteção é inegável. Diversos países já tomaram consciência da importância da segurança em redes de telecomunicações e muitos deles possuem trabalhos específicos sobre o assunto, possuindo inclusive órgãos governamentais responsáveis exclusivamente por essa proteção.

A dimensão em que a segurança é tratada varia de país para país, com alguns abordando as redes de telecomunicações como parte de uma infra-estrutura crítica da informação, o que é justificado pela variedade de serviços básicos que possuem dependência da infra-estrutura de rede: serviços de emergência, sistemas de navegação para tráfego aéreo e entregas, distribuição de energia elétrica e sistemas de controle de água, por exemplo.

Assim, pode-se considerar que serviços básicos são constituídos por infra-estruturas críticas. A definição do que é crítico ou não difere de país para país, podendo ser considerado, de um modo geral, qualquer infra-estrutura que, em caso de algum incidente de segurança, resulta em impactos para a ordem pública, para a saúde pública ou para qualquer tipo de serviço público, como a segurança pública ou a distribuição de energia. Uma dessas infra-estruturas críticas é a de informação, que é uma das principais responsáveis pela integração entre as diferentes infra-estruturas críticas existentes.

A infra-estrutura crítica de telecomunicações, que é discutida neste artigo, é um subconjunto da infra-estrutura crítica de informação (que inclui outros setores como a televisão, rádio ou imprensa), que é um subconjunto da infra-estrutura crítica (que inclui outros setores como a energia, água, saúde ou transporte). Assim, pode-se considerar que a infra-estrutura crítica de telecomunicações é composta por redes como a da telefonia fixa, a da telefonia celular, a de dados, a Internet, de rádio e de satélites.

4. NECESSIDADES DE SEGURANÇA

A natureza da infra-estrutura crítica de um país, com a sua complexidade, convergência e interdependência, faz com que os avisos sejam considerados meros incidentes ou podem realmente se tornar uma situação de crise real?

Existem situações nas quais as redes de telecomunicações possuem um papel fundamental que justifica a necessidade de uma proteção adequada. Em tempos de guerra ou de crise, os adversários podem procurar a intimidação, por exemplo, atacando infra-estruturas críticas e pontos chaves da economia, ou desgastando a confiança pública em sistemas de informação com diferentes tipos de ataques [WHI 03].

Um caso de ataque significativo contra um país ocorreu em 1998: um ataque sofisticado contra a rede de telecomunicações do departamento de defesa americano (*Department of Defense*, DoD), NASA e laboratórios de pesquisa do governo, principalmente contra instituições que realizavam pesquisas sobre segurança nacional, incluindo tópicos sobre atmosfera, oceanografia, design de avião e cabines [WHI 03].

Um outro episódio envolvendo segurança em telecomunicações ocorreu em 1995, quando um grupo denominado "Phonemasters" foi capaz de controlar a rede telefônica da AT&T, Sprint e MCI. O grupo foi capaz de roubar dezenas de milhares de números de cartões telefônicos, encontrar linhas telefônicas privativas da Casa Branca e acessar arquivos confidenciais da FBI. Houve venda dos números de cartões roubados no mercado negro, que incluía clientes como a Máfia Siciliana. Com o ataque, foi possível, por exemplo, redirecionar um número da FBI para uma linha de *sex chat*, o que causou US$ 200 mil em prejuízos. Um fato interessante neste episódio foi o uso, pela FBI, de técnicas para monitorar dados de computadores trafegando via linhas telefônicas [CNN 99].

Considerando o lado da sociedade da informação, a sua própria existência depende das redes cada vez mais complexas e interdependentes e dos serviços baseados na telecomunicação. Logo, se um evento de segurança afeta os negócios e a indústria, bem como os serviços públicos e governamentais, então uma falha em uma infra-estrutura crítica resulta em riscos para a própria sociedade, o que faz com que o assunto seja motivo de preocupação. Assim, novas políticas nacionais devem considerar esse cenário de convergência e interdependência entre infra-estruturas, a vulnerabilidade da sociedade e a sociedade da informação.

Muitos países, como a Holanda, reconhecem a importância da confiabilidade técnica dos sistemas de telecomunicações para a sociedade. Mesmo no âmbito militar, os aspectos de segurança da rede de telecomunicações são um fator chave para vitórias, já que a dependência das forças armadas de tecnologias da informação e comunicação é cada vez maior [LUI 00].

Além da manipulação deliberada de equipamentos de telecomunicações ou sabotagem, os riscos aumentam uma vez que uma determinada infra-estrutura física pode carregar múltiplos tipos de serviços de comunicação, tais como sinais de rádio e televisão, telefonia fixa, telefonia móvel, fax e dados.

É interessante notar que as vulnerabilidades existentes na infra-estrutura de redes estão relacionadas principalmente com a disponibilidade. Perturbações físicas de cabos, intencionais ou não, são os exemplos mais comuns dessa vulnerabilidade. Um caso que ocorreu na Holanda em 1999 envolveu o corte de 4 fibras pertencentes à KPN Telecom em Groningen. O resultado foi a interrupção dos serviços de telefonia móvel e fixo, serviços de alertas, fax, tráfego de dados, Internet e serviços de dinheiro eletrônico, das 8 às 17 horas. Os telefones celulares de concorrentes da KPN também falharam porque uma parte da infra-estrutura de fibra da KPN era compartilhada. Serviços públicos como serviços de licenciamento do governo, polícia e empresas de seguros também ficaram paralisados. Mesmo tendo um *link* emergencial baseado em microondas, o sistema não foi ativado porque não houve reclamações de clientes [LUI 00].

Mesmo o plano de contingência deve ser bem planejado e testado. Um exemplo que demonstrou isso foi a falha na rede *frame relay* da AT&T nos dias 13 e 14 de abril de 1998, na qual a falha na recuperação do desastre e contingência do problema mostrou as fragilidades que podem afetar seriamente um país [NWF 98]. No caso da AT&T, a contingência de sua rede *frame relay* estava na própria rede, ou seja, a contingência real não havia sido planejada.

Com relação à rede de energia elétrica, existem dois fatores que demonstram a sua importância. O primeiro fator é com relação às facilidades de fornecimento de energia emergencial, que podem causar interrupções nas estações base da telefonia celular, por exemplo. Outro fator é que surpresas podem acontecer, mesmo acreditando que sistemas de distribuição de energia estejam em redes isoladas, e portanto inacessíveis para pessoas que estejam fora das estações. Essa foi uma das descobertas feitas em junho de 1997 pelo Pentágono, que com a simulação denominada "Elegible

Receiver", sistemas de controle e monitoramento para distribuição de energia elétrica dos Estados Unidos foram acessados pela Internet.

É preciso analisar, em um país de dimensões continentais como o Brasil, as possibilidades de interrupção dos serviços de telecomunicações.

5. PROTEÇÃO DA INFRA-ESTRUTURA CRÍTICA NA AUSTRÁLIA

A Austrália é um exemplo de país com significativos investimentos do governo em recursos de segurança para sua infra-estrutura crítica. O governo australiano define a infra-estrutura crítica como aquela que, se destruída, degradada ou indisponível por algum intervalo de tempo significativo, traria sérios impactos para a sociedade e economia do país ou problemas para a segurança nacional e defesa [DUN 04].

Recentemente, um estudo baseado na rede de distribuição de energia, em redes de telecomunicações na capital do país, e em suas limitadas conexões com o resto do país, sugeriu que um ataque terrorista contra apenas 3 pontos chaves poderia degradar (possivelmente com severidade) o funcionamento do governo federal, incluindo agências importantes para a segurança nacional [DUN 04]. Além desta, muitas outras vulnerabilidades foram reportadas em estudos similares. O papel do país como um dos principais aliados e parceiros dos EUA justifica toda a preocupação do governo australiano com ataques terroristas contra sua infra-estrutura crítica.

Em Fevereiro de 1997, o DSD (Defence Signals Directorate) publicou um relatório sobre as questões de segurança na infra-estrutura nacional de telecomunicações da Austrália [DSD 97]. A principal recomendação era o estabelecimento de uma estrutura formal para coordenar e implementar uma política nacional para proteção para a chamada NII (National Information Infrastructure), envolvendo o governo e o setor privado. Recomendações suplementares cobriam a necessidade de classificação da informação, criação de níveis adequados de conscientização e proteção, o estabelecimento de um CERT (Computer Emergency Response Team) nacional e criação de uma equipe responsável por fazer análises de vulnerabilidades [ICP 98].

Como resultado deste relatório, o governo australiano promoveu um fórum com a comunidade e o setor privado e chegou à conclusão de que todas as recomendações, apresentadas no relatório do DSD, deveriam ser implementadas. Isto culminou com a criação do NIIPS (National Information Infrastructure Protection Secretariat), que ficou responsável pela implementação das medidas necessárias para a proteção das redes de telecomunicações do país.

Os ataques de 11 de Setembro de 2001, nos EUA, e de 12 de Outubro de 2002, em Bali, fizeram com que o governo australiano voltasse a avaliar políticas e planos de segurança nacionais e leis. Algumas mudanças foram realizadas, buscando minimizar as ameaças do terrorismo. Merecem destaque todas as reformas feitas na legislação do país, tal como a inclusão do "Cybercrime Act" (2001). Em 2003, foram criados: o "National Counter-Terrorism Plan", o TISN ("Trusted Information Sharing Network for Critical Infrastructure Protection") e o AHTCC ("High Tech Crime Centre") [DUN 04].

A Austrália é um dos países participantes do mítico projeto de espionagem Echelon, apesar de ser proibido, neste país, interceptar comunicações através do ato "Telecommunications (Intercepetion) Act 1979" (exceto em casos onde há autorização legal explícita). O Echelon é, talvez, a mais poderosa organização de inteligência, em telecomunicações, do mundo. Diversos relatórios sugerem a existência de um sistema global de vigilância ("surveillance system") capaz de obter informações em diversos canais de telecomunicações, em todo o mundo. De acordo com tais relatórios, o Echelon tenta capturar comunicações via satélite, microondas, telefonia celular e fibra-óptica. Por meio de sofisticadas tecnologias de filtragem, baseadas em inteligência artificial, padrões específicos são identificados nas comunicações [ECH 04].

A criação de projetos de espionagem em tráfegos de redes de telecomunicações tem se tornado uma prática comum em muitos países do mundo. Agências de Inteligência estão cada vez mais preocupadas em buscar informações nestes tráfegos para combater o terrorismo, espionar outros países ou para fins de contra-inteligência.

6. PROTEÇÃO DA INFRA-ESTRUTURA CRÍTICA DE TELECOMUNICAÇÕES NA CHINA

Na China, as questões de segurança relacionadas às redes de telecomunicações dizem respeito, principalmente, à censura do tráfego de informações, que busca evitar a propagação de propaganda política contrária ao regime vigente, à segurança nacional e à "*Information Warfare*". Este último interesse não é confirmado. Todavia, segundo o serviço de inteligência americano, CIA, há atividades desenvolvidas e financiadas pelo governo chinês com o objetivo de desenvolver pessoal qualificado em segurança, técnicas e ferramentas para fins bélicos contra outros países [COM 00] [SIL 02], em especial contra os EUA. Isto pode constituir um novo campo de batalha, onde ataques remotos podem ser realizados, sem perdas humanas e com grande eficácia, atingindo serviços vitais do inimigo.

Desde que o uso da Internet foi permitido na China, em 1995, todos os acessos a serviços têm sido redirecionados para servidores do governo, onde administradores criteriosamente bloqueiam acesso a endereços de servidores de notícias ocidentais, endereços de servidores de dissidentes políticos chineses, jornais de Taiwan (por se tratar de uma "província" considerada rebelde pelo governo chinês) e outros materiais considerados "perigosos" à saúde do regime [CPJ 01] [POL 00]. Como parte deste esforço, uma agência de polícia e inteligência especial foi criada, em 1998, com objetivos de vigilância na Internet, para rastrear dissidentes políticos e conduzir espionagem contra estrangeiros. Portanto, a idéia principal é proteger o regime político do país contra qualquer ameaça capaz de desestabilizá-lo.

Uma iniciativa do governo chinês é desenvolver um sistema anti-satélite (ASAT). A China, desta forma, é o terceiro país a ter tal sistema. Os outros dois são os EUA e a Rússia. O objetivo deste projeto é criar "*parasitic sattelites*", capazes de gerar interferência ou destruir satélites de inimigos [CHE 00]. Isto, dentre outras coisas, impede a atuação dos chamados "satélites espiões".

Por se tratar de um país extremamente fechado, não há muitas informações detalhadas sobre como este país está tratando das questões de segurança em redes de telecomunicações. Contudo, fica claro o forte controle do governo chinês sobre o setor de telecomunicações e as informações que entram e saem do país. Um aspecto marcante é a rígida censura imposta pelo governo aos cidadãos chineses e a ausência de privacidade no uso da Internet, para manutenção do regime político.

7. CONTEXTUALIZAÇÃO DO BRASIL

O Brasil, com todas suas peculiaridades, ameaças e interesses próprios, deve criar uma estratégia de segurança mais adequada para o país. Obviamente, as idéias e similaridades de outros países, tais como estes que foram discutidos ao longo deste artigo, devem ser aproveitadas para a formatação de uma solução nacional. As questões de soberania nacional, principalmente, devem ditar os caminhos a serem trilhados pelo Brasil em busca de uma solução de segurança nacional.

Considerando o caso particular da infra-estrutura crítica de telecomunicações, há ainda várias ameaças a serem identificadas, mapeadas e tratadas pelo governo brasileiro, de forma a garantir os interesses da nação e dos seus cidadãos.

O Brasil, por sua importância estratégica e posição de liderança na América Latina, é um país que precisa oferecer um tratamento adequado para todas as suas infra-estruturas críticas, em especial, sua infra-estrutura de telecomunicações. Já há algumas iniciativas do governo brasileiro, mas muito trabalho ainda precisa ser realizado. O Decreto 3505, de 13 de Junho de 2000, institui a política de segurança da informação nos órgãos e entidades da Administração Pública Federal [PLA 04]. Contudo, esta ainda não está sendo implementada como deveria.

A Câmara Técnica dos Serviços de Rede do Poder Executivo criou o Grupo de Segurança da Informação. Este grupo foi consolidado, no ano 2000, com a formação do Comitê Gestor de Segurança da Informação (CGSI) [PLJ 04]. Além dos membros do CGSI, o Brasil conta com a participação técnica de algumas instituições tais como o CEPESC (Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações) e os centros de respostas a incidentes brasileiros CAIS/RNP [RNP 04]

e NBSO [NBS 04](estes dois centros são os únicos brasileiros membros do FIRST). O CEPESC é integrante da estrutura do Departamento de Tecnologia da ABIN (Agência Brasileira de Inteligência).

Mais recentemente, em 24 de Março de 2004, o governo federal baixou a portaria normativa 333 [MID 04], do Ministério da Defesa, que institui a Política de Guerra Eletrônica de Defesa.

Portanto, há alguns esforços no sentido de melhorar os níveis de proteção às infra-estruturas críticas do país, sob uma predominante perspectiva de soberania nacional. Notar que os interesses e preocupações são outras. O Brasil não sofre ameaça iminente do terrorismo internacional, não busca controlar uso dos sistemas de telecomunicações para inibir propaganda política, etc. Portanto, o cenário é diferente e as estratégias devem se acomodar a esta realidade. A principal preocupação do governo brasileiro é proteger as informações estratégicas do país.

8. SEGURANÇA DA INFRA-ESTRUTURA DE TELECOMUNICAÇÕES DO PAÍS

O Brasil apresenta um cenário de telecomunicações bastante peculiar e complexo. Todo o sistema de telecomunicações do país está nas mãos do setor privado e, em sua maioria, sob o controle de grandes grupos internacionais. Notadamente, os sistemas de telefonia fixa e móvel estão nas mãos de europeus e americanos. Tais países podem tirar proveito desta situação para levar vantagens econômicas, políticas e comerciais junto ao Brasil. A possibilidade de interferências externas de outros países é grande, uma vez que informações estratégicas para o país podem estar trafegando por tais redes. Além disto, indisponibilidades (ou mau funcionamento) temporárias ou permanentes, nestas redes, podem trazer sérias conseqüências ao país, podendo afetar toda a população.

O setor de telecomunicações tem evoluído constantemente no Brasil e no mundo, resultando em muitas mudanças de paradigmas. Essas mudanças são frutos da evolução e inovação tecnológica capazes de criar novas oportunidades de negócios não somente para o setor, mas também para praticamente todos os setores da economia. Alguns exemplos de tecnologias de ruptura são a telefonia móvel celular, a Internet, a TV digital e as redes Ad-Hoc.

No Brasil, a evolução do setor de telecomunicações ocorreu mais fortemente a partir de meados da década de 60, como braço de execução de uma política nacional que considerava as comunicações como estratégicas para o desenvolvimento e a integração do País [MCT 02]. Nessa época, a telefonia fixa possuía um papel fundamental, e a partir da década de 90 a digitalização de linhas e sistemas foi acompanhada do surgimento de novas tecnologias e produtos de comunicação baseados em novas linguagens e protocolos. Alguns destaques foram os serviços móveis celulares e a Internet, que possibilitaram a criação de diversos serviços que possuem um valor incontestável para os objetivos do governo.

9. OUTROS TRABALHOS

Um dos trabalhos que vem sendo desenvolvido para a evolução da proteção da infra-estrutura crítica de telecomunicações é a definição de uma metodologia para identificação e avaliação de riscos envolvidos.

Paralelamente, a definição de um cenário ideal para a segurança em telecomunicações resulta em grandes benefícios não apenas para o Brasil, mas também para todos os interessados em organizar os aspectos de segurança envolvidos.

Identificando as ameaças e as vulnerabilidades, a intenção do trabalho é prover uma visão estruturada dos riscos reais existentes que devem ser considerados no contexto de uma sociedade da informação confiável e quais as responsabilidades do governo. O fato é que muitas infra-estruturas estão nas mãos do setor privado ou em mãos estrangeiras, o que agrava o problema de demarcação de limites. Isso reforça o lado regulatório e o lado de interação e cooperação nacional, o que eleva o problema à esfera política, além do tecnológico. O objetivo é estabelecer uma estratégia que faça com que as redes de telecomunicações funcionem adequadamente, com a minimização da interferência de problemas naturais ou ambientais, erros humanos e operacionais ou ataques maliciosos.

10. CONCLUSÃO

A preocupação com a segurança da infra-estrutura de telecomunicações é um fato concreto em diversos países, como foi possível verificar neste artigo. A importância de se abordar a segurança da rede de telecomunicações pode ser comprovada pelas iniciativas que estão sendo tomadas em diversos países, com a criação de órgãos específicos para tratar o tema.

A contextualização do Brasil no cenário mundial mostra que o país deve tratar a segurança da rede nacional de telecomunicações com bastante seriedade, já que o estudo de diferentes países mostrou essa tendência. De fato, entender o que outros países vêm realizando para a proteção da rede de telecomunicações é fundamental tanto para o direcionamento das ações do Brasil, bem como para a cooperação, que é parte importante da estratégia de qualquer país.

É preciso entender ainda, como foi discutido neste artigo, que o Brasil possui um contexto diferente dos países analisados, o que reforça a análise das particularidades brasileiras e dos riscos existentes para o Brasil.

11. REFERÊNCIAS BIBLIOGRÁFICAS

[ABI 04] http://www.abin.gov.br/abin/cepesc_abertura.jsp

[APE 99] "Internet PKI Applications in Chinese Taipei". Submit to APEC TEL 19th Meeting, Taiwan, 1999. http://www.apectelwg.org/apecdata/telwg/19tel/bfsg/bfsg-14.pdf

[CHE 00] Ho, C. "China Eyes Anti-Satellite System". Spacedaily. Janeiro de 2000. http://www.spacedaily.com/news/china-01c.html

[COL 03] COLLEGE, Marist; NAKRA, Prema. Journal of Competitive Intelligence and Management. Volume 1, Number 2, Summer 2003.

[COM 00] McCathy, J. "CIA: China, Rússia develop cyberattack capability". IDG News Service, 2000. http://www.computerworld.com/news/2000/story/0,11280,41476,00.html.

[CNN 99] CNN.com. Large-Scale Phone Invasion Goes Unnoticed By All But FBI. http://www.cnn.com/1999/TECH/computing/12/14/phone.hacking/ . December 14, 1999

[CPJ 01] Neumann, L. "The Great Firewall". Janeiro de 2001. http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html

[DSD 97] "Australia's National Information Infrastructure: Threats and Vulnerabilities". Defense Signals Directorate (DSD). Fevereiro de 1997.

[DUN 04] Dunn, M.; Wigert, I. "International CIIP Handbook 2004". Centro para Estudos de Segurança. Instituto de Tecnologia Federal da Suíça. Zurique 2004.

[ECH 04] http://archive.aclu.org/echelonwatch/

[EPI 02] "Privacy and Human Rights: An International Survey of Privacy Laws and Developments". Privacy International and the Electronic Privacy Information Center (EPIC). 2002.

[FAZ 04] http://www.fas.org/irp/world/china/mps/org.htm

[FST 04] http://www.first.org

[GLO 04] GlobalSecurity.org. Research And Analysis Wing [RAW]. http://www.globalsecurity.org/intell/world/india/raw.htm.

[GEO 03] "G8 Principles for Protecting Critical Information Infrastructures", G8 Justice & Interior Ministers, Maio de 2003.

[ICP 98] "Protecting Australia's National Infrastructure". Interdepartmental Committee on Protection of the National Infrastructure. Canberra, Dezembro de 1998.

[ICPNI 98] Protecting Australia´s National Information Infrastructure. Report of the Interdepartamental Committee on Protection of the National Infrastructure. Attorney-General´s Departament, Canberra, Dezembro de 1998.

[ITU 02] International Telecommunication Union. International Coordination To Increase The Security Of Critical Network Infrastructures. ITU Workshop On Creating Trust In Critical Network Infrastructures. Seoul, Republic of Korea. May 2002, 20-22.

[LUI 00] LUIIJF, H.A.M.; KLAVER, M.H.A. In Bits and Pieces. Vulnerability Of The Netherlands Ict-Infrastructure And Consequences For The Information Society. March 2000.

[LUK 03] Lukasik, S.; Goodman, S. "Protecting Critical Infrastructures Against Cyber-Attack". International Institute for Strategic Studies. ADELPHI PAPER 359. 2003.

[MCT 02] Ministério da Ciência e Tecnologia. Programa Sociedade da Informação. Sociedade da Informação no Brasil - Livro Verde. Anexo 3 – Informática e Telecomunicações no Brasil. http://www.mct.gov.br/Temas/Socinfo/Livro_Verde/ca03.pdf.

[MID 04] Portaria Normativa 333/MD. DOU, Edição Número 59, Março de 2004.

[NBS 04] http://www.nbso.nic.br

[NWF 98] ROHDE, David. Network World. Why At&T's Disaster Recovery Service Failed. http://www.nwfusion.com/news/0427frame2.html. April 27, 1998.
[NAK 03] NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. Segurança de Redes em Ambientes Cooperativos – 2ª Edição. Editora Futura, 2003.
[OCI 04] http://www.ocipep.gc.ca/home/index_e.asp
[PEO 00] "China Defines Qualifications Of Basic Telecom Operators". People's Daily. Outubro de 2000. http://fpeng.peopledaily.com.cn/200010/25/eng20001025_53558.html
[PLA 98] PALÁCIO DOS PLANALTOS. Mensagem Ao Congresso Nacional 1998 - Parte IV - Infraestrutura. Na Abertura da 4ª Sessão Legislativa Ordinária da 50ª Legislatura. https://www.planalto.gov.br/publi_04/COLECAO/98MENS4B.HTM.
[PLA 04] https://www.planalto.gov.br/gsi/cgsi/
[PLJ 04] http://www.planejamento.gov.br
[POL 00] Recio, E. "The Great Firewall of China: Cyber-Censorship". 2000. http://polywog.navpoint.com/sociology/devnat/firewall_of_china/
[RNP 04] http://www.rnp.br/cais/sobre.html
[SAN 97] SANGHVI, Vir. Who Decides Whose Phone Is To Be Tapped? http://www.rediff.com/news/apr/02vir.htm.
[SIL 02] Lichtblau, E. "CIA: China planning cyber-attacks on U.S". 24 de Abril de 2002. http://www.siliconvalley.com/mld/siliconvalley/3132466.htm?template=contentModules/printstory.jsp
[TWH 03] The National Strategy to Secure Cyberspace. The White House. Fevereiro de 2003.
[WHI 03] The White House, Washington. The National Strategy To Secure Cyberspace. February, 2003.
[ZET 04] ZETTER, Kim. Wired News. Virus Alert Program Debuts. January 28. 2004. http://www.wired.com/news/business/0,1367,62078,00.html.

COMBATENDO CRIMES DIGITAIS COM SISTEMAS DE *SURVEILLANCE*

Marcelo Barbosa Lima, Emilio Tissato Nakamura,

Edson Kowask Bezerra, Sérgio Luís Ribeiro

CPQD - Centro de Pesquisa e Desenvolvimento - Telecom & IT Solutions
Rod Campinas – Mogi-Mirim, km 118,5 – SP340 – CEP 13086-902 – Campinas/SP
{kowask, nakamura, mlima, sribeiro}@cpqd.com.br

Abstract

This article aims at showing an idea to make easier the forensic investigation of digital crimes in the Brazilian Internet, using a surveillance system. This project is a starting work. So, many details still need be studied and better specified. Besides, privacy and laws issues are quickly discussed in this paper too.

1. INTRODUÇÃO

O Brasil tem sido reconhecido como um dos maiores celeiros de *crackers* do mundo. A ausência de uma legislação específica para tratamento aos crimes digitais, bem como as facilidades oferecidas, aos usuários maliciosos da Internet brasileira, contribuem para esta fama. Isto pode ser comprovado pelo grande número de "grupos *hackers*" atuando impunemente no país. Há alguns anos, tais grupos restringiam suas atividades a ataques de *defacements* de *sites* na *Web* (pichar páginas em servidores *Web*).

A evolução da Internet e o crescimento das operações comerciais e financeiras, pela rede, criaram uma nova realidade. Várias ameaças surgiram, usuários maliciosos e grupos criminosos perceberam que diversas vulnerabilidades poderiam ser exploradas facilmente sem riscos de serem descobertos. Isto sem falar na própria legislação, que deixa várias lacunas abertas ou mal resolvidas. O resultado é que hoje a Internet é um ambiente bastante inóspito com diversos ataques cada vez mais sofisticados. Isto justifica a rápida proliferação de atividades criminosas na rede. Atividades que vão de pornografia infantil até fraudes financeiras.

Este trabalho tem como objetivo mostrar uma possível solução para combate a diversos tipos de crimes digitais. A solução é complexa, envolve diferentes atores e uma legislação apropriada. Trata-se da concepção de um sistema de *surveillance* nacional para combate a crimes virtuais.

2. CRIMES DIGITAIS NO BRASIL

Com base nos últimos acontecimentos, temos percebido que definitivamente o crime organizado começou a voltar a sua atenção para a Internet. Percebeu-se que alguns tipos de crimes, que antes envolviam grandes operações e riscos físicos, poderiam ser feitos sem muitos problemas por meio da Internet. Isto sem falar que os ganhos obtidos podem ser, na maioria das vezes, bem maiores. Um exemplo interessante é o ataque de *phishing* SCAM [1], onde grupos criminosos iludem correntistas de bancos populares do país.

Neste tipo de ataque, as únicas armas usadas pelo criminoso são um *e-mail* enviado para diversos usuários na Internet e um servidor clone do *site* de um banco (em geral, um grande banco popular do país). Este servidor está localizado geralmente em alguma máquina comprometida em

outro país. O combate a este tipo de crime tem sido bastante difícil: não é simples rastrear as origens dos *e-mails* e os servidores usados são comprometidos. Além disto, há a falta de colaboração de polícias e leis internacionais para crimes digitais.

O *e-mail* tem como objetivo básico iludir usuários, induzindo-os a acessarem o servidor controlado pelo grupo criminoso. As páginas visualizadas em tal servidor são cópias perfeitas das páginas originais do banco. O ataque é bem sucedido quando usuários informam dados sobre suas contas correntes, incluindo as senhas. O grupo pode coletar um número significativo de senhas para acesso legal aos servidores reais do banco e realizar transferências financeiras para contas dos chamados "laranjas". Isto dificulta o rastreio do dinheiro no sistema financeiro brasileiro.

O grande problema, que facilita esta atividade criminosa, é a falta de uma cultura em segurança. Este tipo de ataque se utiliza basicamente de engenharia social, onde usuários acreditam no *e-mail* (geralmente com promoções especiais) e utilizam um *link*, no corpo da mensagem, para acesso ao servidor do banco. Há algumas técnicas para fazer o *link* parecer ser um endereço real do banco, codificando o real endereço do servidor usado pelo grupo. Isto dificulta que usuários menos crédulos percebam o golpe. Outro fato que demonstra esta falta de cultura é que usuários não verificam a autenticidade do certificado digital do servidor (muitas vezes, sequer verificam a existência de um certificado digital).

A Internet também propicia uma forma mais rápida de distribuição de pornografia infantil e atividades relacionadas à pirataria [2] (*softwares*, livros, músicas, filmes, etc.). Estas atividades criminosas não são exclusividades do Brasil. A tarefa de rastrear os responsáveis é sempre dificultada, pois o material ilegal é sempre disponibilizado em servidores comprometidos localizados nos mais variados lugares do mundo ou por meio de *softwares* P2P de compartilhamento de arquivos.

Outra ameaça para usuários, quando utilizando o servidor de um banco na Internet, é ter suas senhas roubadas através de ferramentas especiais capazes de registrar todas as teclas pressionadas por um usuário, durante o acesso ao servidor do banco. Tais ferramentas são chamadas de "*key loggers*". O desafio para o grupo criminoso é instalar esta ferramenta nos computadores das vítimas. Mas várias estratégias podem ser utilizadas para este fim: através de SPAM com o arquivo anexado, usando cavalos de Tróia, etc. As senhas podem ser obtidas por *e-mail*, por acesso do usuário malicioso via *backdoor*, etc. Este tipo de fraude também é difícil de rastrear, visto que raramente a máquina de um usuário é verificada , após um incidente. Isto sem falar nas diversas técnicas usadas por criminosos para esconder as trilhas deixadas.

Para combater este problema, bancos passaram a utilizar os chamados "teclados virtuais" [3], evitando que usuários usem o teclado convencional para digitar senhas e outras informações secretas. Todavia, isto motivou a criação das ferramentas de "*screen loggers*", que registram todas as ações realizadas pelos usuários utilizando o *mouse*. Tais ferramentas são capazes de armazenar um determinado intervalo de imagens de porções da tela, capturadas durante o uso do teclado virtual. Portanto, as senhas podem ser obtidas por meio deste *malware*.

Outro ataque que tem como alvo correntistas de um banco implementa um *Man-In-The-Midlle* (MITM) [4]. Uma máquina sob controle do criminoso é colocada no meio do caminho entre o servidor real e um cliente. Isto é feito por meio de uma alteração na configuração padrão do navegador dos usuários: o navegador é configurado para usar um *proxy* sob controle dos criminosos. Trata-se, portanto, de mais um ataque ativo, onde a configuração especial pode ser feita por meio de uma *backdoor* instalada no sistema da vítima. Em geral, o servidor *proxy* usado pelo criminoso é uma máquina comprometida em qualquer parte do mundo.

Uma outra modalidade de crime praticado por meio da Internet é a extorsão. Esta modalidade de crime ainda não é muito comum no Brasil. Mas já há casos sendo investigados pelo FBI nos EUA. Este tipo de crime tem como alvo uma instituição ou pessoa dentro de uma instituição. Neste caso, o criminoso ameaça realizar algum ataque contra uma instituição (na maioria dos casos, os ataques são de *Denial-of-Service*), caso não receba uma certa quantia em dinheiro. Como o contato, na maioria dos casos, ocorre por telefone, a polícia tem dificuldade para identificar o autor.

Como o leitor pode observar, há vários tipos de fraudes e crimes praticados usando a Internet. Os poucos ataques citados nesta seção fazem parte de um grupo muito maior de atividades criminosas. Muitos destes crimes abusam da boa fé e ingenuidade dos usuários. A falta de uma cultura de segurança é a principal vulnerabilidade explorada na grande maioria destes ataques. A solução,

embora pareça simples, é extremamente complexa. Criar uma cultura de segurança digital em âmbito nacional/internacional é uma tarefa complexa.

Um maior nível de proteção poderia ser utilizado em sistemas operacionais. Contudo, desenvolvedores de tais sistemas não acham interessante elevar o grau de dificuldade para operação do sistema. Sistemas operacionais comerciais tendem a serem cada vez mais "amigáveis", permitindo que qualquer pessoa seja capaz de utilizar o computador. Mecanismos de proteção, em geral, adicionam dificuldades adicionais para configuração destes sistemas. Utilizar softwares de proteção, fornecidos por bancos, não são vistos com bons olhos por gerentes destas instituições, pois trazem altos custos adicionais com suporte.

Por outro lado, o trabalho da polícia é sempre dificultado. A ausência de colaboração e a falta de registros e *logs* são aspectos importantes. A tarefa de identificar o criminoso na rede é bastante complexa e temos registrado alguns poucos casos de sucesso. Sistema de vigilância na Internet poderia oferecer um grande número de evidências para um investigador forense. Possibilitaria encontrar um criminoso no momento inicial de suas atividades. Os autores acreditam que tal sistema possibilitaria aumentar consideravelmente a probabilidade de sucesso em investigações de crimes praticados via Internet.

3. PROJETOS DE SURVEILLANCE AO REDOR DO MUNDO

Vários países já contam com projetos de *surveillance*. Na maioria dos casos, entretanto, estes sistemas são usados pelas agências de inteligência para espionagem de outros países ou combate ao terrorismo. Vários destes sistemas são guardados como segredos por governos, uma vez que estão relacionados a assuntos de segurança nacional.

Um dos projetos mais famosos é o lendário Echelon [5]. Participam do Echelon os países de língua inglesa: os EUA, a Austrália, o Reino Unido, o Canadá e a Nova Zelândia. O Echelon é, talvez, a mais poderosa organização de inteligência, em telecomunicações, do mundo. Diversos relatórios sugerem a existência de um sistema global de vigilância capaz de obter informações em diversos canais de telecomunicações, em todo o mundo. O grande objetivo de tal sistema é a espionagem.

De acordo com tais relatórios, o Echelon tenta capturar comunicações via satélite, microondas, telefonia celular e fibra-óptica. Por meio de sofisticadas tecnologias de filtragem, baseadas em inteligência artificial, padrões específicos são identificados nas comunicações. Informações reais sobre tal projeto não são conhecidas. O governo americano sequer admite a existência do Echelon. Contudo, governos da Austrália e da Nova Zelândia já confirmaram a existência do projekto. A figura abaixo tenta descrever o que seria o projeto Echelon [6].

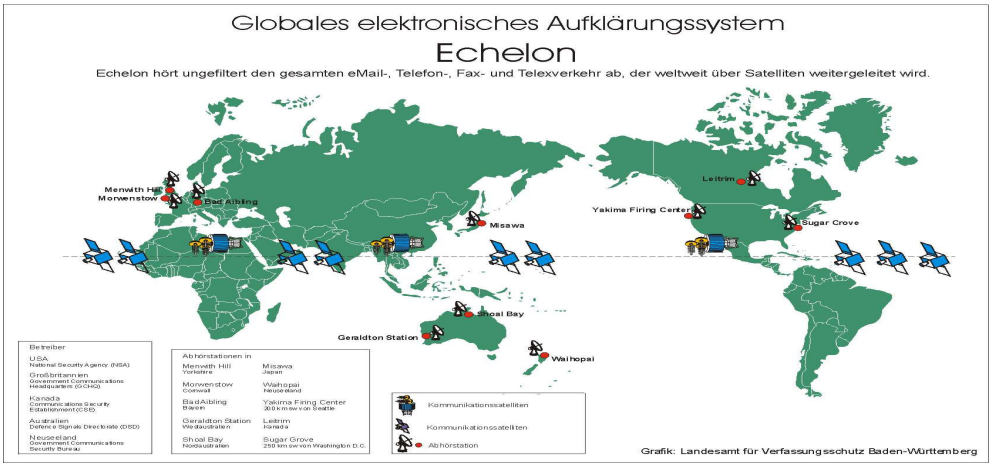


Figura 1: Visão Hipotética do Projeto Echelon

Outros países que contam com projetos de *surveillance* em redes de dados e telecomunicações em geral, com objetivos específicos de espionagem interna, espionagem de outros países e de grupos terroristas são a Rússia, a China, a Alemanha, Israel, França e Índia. Alguns destes sistemas também são utilizados no combate ao crime [6].

Por outro lado, sob a perspectiva de combate a crimes no âmbito nacional, nos EUA há um outro projeto conhecido como "Carnivore" [7] (atualmente, fala-se no "Altivore" que aumenta as capacidades do Carnivore). O Carnivore é uma ferramenta de interpecção de tráfego de rede usada, pelo FBI, para combater o terrorismo, o tráfico de drogas e atividades maliciosas na rede. Ele permite a coleta de evidências criminais, buscando provas na rede. Dentre outras coisas o Carnivore/Altivore permite: monitoramento de *e-mails* individuais, monitoramento de acessos a certos serviços (FTP, HTTP, etc.) e descoberta de endereços IP de um determinado indivíduo para interceptar todo o tráfego relacionado.

O Carnivore é usado em grandes ISP (*Internet Service Provider*), sob forte protesto dos defensores da privacidade individual. Baseado no suporte legal necessário, o FBI solicita a instalação do Carnivore para que seja possível fazer a investigação nas comunicações eletrônicas de suspeitos. Ao contrário do Echelon, este sistema é bem conhecido e confirmado pelas autoridades americanas.

Um cenário interessante ocorre na África do Sul [8]. Neste país, provedores de telecomunicações são obrigados, por lei, a fornecerem canais de comunicação para um centro de monitoramento nacional, permitindo que tráfego especial seja interceptado. As operadoras não podem oferecer qualquer tipo de serviço que não permita eventual monitoramento. O acesso anônimo a serviços de telecomunicações é proibido no país. O governo se encarrega de criar os vários centros de monitoramento. O objetivo principal desta estratégia é o combate à criminalidade crescente no país.

Podemos citar ainda o caso da China [9]. Desde que o uso da Internet foi permitido na China, em 1995, todos os acessos a serviços têm sido redirecionados para servidores do governo, onde administradores criteriosamente bloqueiam acesso a endereços de servidores de notícias ocidentais, endereços de servidores de dissidentes políticos chineses, jornais de Taiwan (por se tratar de uma "província" considerada rebelde pelo governo chinês) e outros materiais considerados "perigosos" à saúde do regime. Todas estas atividades são consideradas ilegais na China. Como parte deste esforço, uma agência de polícia e inteligência especial foi criada, em 1998, com objetivos de vigilância na Internet, para rastrear dissidentes políticos e conduzir espionagem contra estrangeiros.

4. USO DE SISTEMAS DE SURVEILLANCE PARA COMBATE A CRIMES DIGITAIS NO BRASIL

A idéia deste trabalho é propor um projeto similar para a Internet brasileira. O país deve investir em mecanismos/tecnologias para combater as atividades criminosas realizadas pela rede. Isto deve ser feito antes que outros países comecem a aumentar o controle e filtragem do tráfego originado no país, isolando cada vez mais a Internet brasileira. Um sistema de vigilância eletrônico seguindo o modelo do Carnivore parece ser uma solução bastante interessante para o país. Isto significa que um conjunto de normas específico precisa ser criado para provedores Internet brasileiros.

Uma outra importante justificativa para a facilidade de realização de atividades criminosas, pela Internet, é a quase total ausência de mecanismos de controle nos provedores de acesso existentes no país. Usuários podem, por exemplo, usar técnicas de IP *spoofing* para diminuir a possibilidade de serem rastreados pela polícia. Alguns provedores não mantêm *logs* muito detalhados dos acessos de cada usuário. Aliado aos problemas técnicos, o Brasil ainda não conta com uma legislação específica para tratamento dos crimes praticados por computador.

A proposta deste trabalho é a criação de centros de monitoramento, similares àqueles usados na África do Sul, e a utilização de tecnologias de monitoramento, que chamaremos de "SnifferBox", a serem introduzidas em provedores Internet brasileiros. As informações relevantes, coletadas por cada SnifferBox, individual devem ser enviadas para centros de monitoramento regionais, onde podem ser usados por investigadores das Polícias Federal e/ou Civil. O tráfego deve ser encaminhado por meio

de túneis seguros VPN, para evitar que as informações possam ser obtidas/manipuladas por pessoas não autorizadas.

Toda uma inteligência deve ser criada em uma SnifferBox. Na prática, ela deve ter a capacidade de coletar todo o tráfego e buscar padrões que possam caracterizar uma atividade maliciosa. Técnicas de inteligência artificial podem ser utilizadas na implementação do módulo de busca de padrões. Em paralelo, certas informações de *log* do provedor também podem ser redirecionadas para uma SnifferBox. O ideal é que apenas o tráfego relativo ao usuário suspeito seja monitorado por questões de privacidade e desempenho.

Isto facilita determinar a fonte de ataques, no momento em que o crime é realizado. Além disto, o usuário pode ser identificado por meio das informações passadas durante o processo de autenticação. Tais *logs* são redirecionados para SnifferBoxes. Isto significa que o processo de assinatura em provedores deve ser mais rigoroso quanto à documentação dos usuários.

Contudo, há casos onde o acesso à Internet é disponibilizado sem custos e sem necessidade de inscrição dos usuários. Nestes casos, um esquema deve ser usado para permitir o rastreio do usuário por meio do número de telefone usado. A figura abaixo ilustra o cenário proposto.

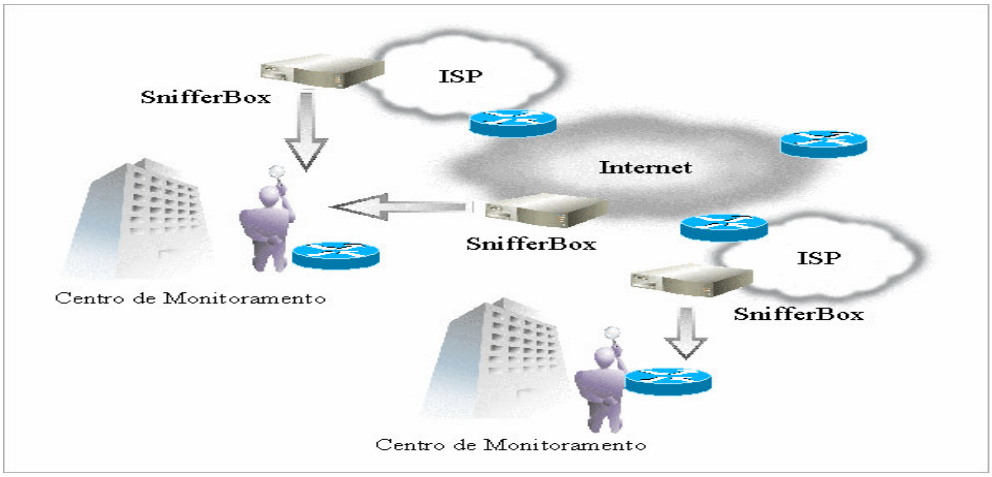


Figura 2: Distribuição de SnifferBoxes e Centros de Monitoramento.

5. DESAFIOS DO PROJETO DE SURVEILLANCE

O projeto apresenta vários desafios, conforme o leitor pode ter observado. Um deles está relacionado às questões de privacidade. A SnifferBox deverá ser capaz de inspecionar todo o tráfego, sem relacioná-lo a qualquer usuário específico. Apenas após um padrão ser identificado, o tráfego relativo a usuários suspeitos deve ser interceptado.

Outro grande desafio é o tráfego cifrado. Todavia, isto não chega a ser um problema para detectar a maioria dos ataques realizados por criminosos cibernéticos, uma vez que criptografia não é utilizada nas atividades mencionadas neste documento. Para simplificar o projeto da tecnologia de monitoramento, é recomendável que tráfego cifrado seja simplesmente ignorado pelo sistema de vigilância eletrônico.

Um conjunto de normas específicas para provedores Internet precisa ser criado de antemão. Eles deverão inserir SnifferBoxes em suas respectivas infra-estruturas de rede. Além disto, algumas informações de *logs*, geradas em diversos pontos da rede, devem ser enviadas para SnifferBoxes também. Portanto, algum mecanismo de *enforcement* precisa ser criado para garantir a perfeita operação do sistema.

Esta proposta envolve algum investimento extra. Centros de monitoramento devem estar conectados a todos os provedores de uma região. Além disto, várias SnifferBoxes podem ser necessárias em certos provedores Internet.

6. CONCLUSÃO

Este trabalho tem como objetivo propor a criação de um grande sistema de *surveillance* na Internet brasileira. Tal sistema seria criado para o combate ao crime digital cada vez mais organizado e sofisticado. Por se tratar de uma proposta ainda incipiente, o documento não apresenta muita riqueza de detalhes de implementação do sistema.

Contudo, o grande desafio reside no fato que uma regulamentação deve ser criada para que provedores Internet brasileiros possibilitem a instalação e operação de componentes do sistema. As questões de privacidade individual devem ser tratadas de forma cuidadosa, para evitar problemas com as leis de defesa da privacidade do cidadão.

Acredita-se que, inspecionando todo o tráfego em determinados pontos da rede, é possível detectar diversos tipos de ataques comuns na Internet. O combate ao crime pode ser mais efetivo com esta ferramenta, uma vez que a origem e autoria das atividades poderão ser definidas.

7. REFERÊNCIAS

[1] http://www.antiphishing.org/
[2] http://www.abes.org.br/antipirataria/index.htm
[3] http://www.naveguemelhor.com.br/especial/default.asp?ID=777
[4] www.invasao.com.br/coluna-marcos-13.htm
[5] http://www.echelonwatch.org/
[6] http://www.fas.org/irp/program/process/echelon.htm
[7] http://www.robertgraham.com/pubs/carnivore-faq.html
[8] "***Republic Of South Africa Interception And Monitoring Bill***". Government Gazette, 2001.
[9] Recio, E. "*The Great Firewall of China: Cyber-Censorship*". 2000.
http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html

LA EXPLOTACIÓN SEXUAL COMERCIAL INFANTIL EN INTERNET

Dra. Yalena de la Cruz[1]

Abstract

Las personas nos organizamos en la sociedad para maximizar nuestro bienestar. No obstante, suelen ocurrir, en nuestros espacios de interrelación, abusos o excesos, muchas veces producto de un ejercicio irresponsable de la libertad con el que se irrespeta o lesiona a los demás, con faltas, contravenciones, delitos, agresiones, etc.. La Internet, como espacio de interrelación social, es también una plataforma para delinquir. Como toda herramienta, no ha podido escapar de los usos perversos, entre los que encontramos la explotación sexual comercial infantil, que se aborda en este artículo desde la perspectiva de proteger el interés superior de los niños, niñas y adolescentes.

1. INTRODUCCIÓN

Las personas nos organizamos en la sociedad para maximizar nuestro bienestar. No obstante, suelen ocurrir, en nuestros espacios de interrelación, abusos o excesos, muchas veces producto de un ejercicio irresponsable de la libertad con el que se irrespeta o lesiona a los demás, con faltas, contravenciones, delitos, agresiones, etc.. La Internet, como espacio de interrelación social, es también una plataforma para delinquir. Como toda herramienta, no ha podido escapar de los usos perversos, entre los que encontramos: intrusiones (hacking y robo de información) y ataques (cracking, virus y gusanos), o utilizada (fraude con tarjetas de crédito, phishing con ventas fraudulentas en portales www falsos, phreaking con líneas telefónicas "gemeleadas", pornografía infantil, propiedad intelectual, robo de señal satelital y otros).

Para quienes defendemos el interés superior de los niños en la vida social, es vital controlar los delitos contra los menores en el ciberespacio, entre los encontramos lo que se denomina "erótica infantil", es decir, cualquier artículo (para ver en pantalla o vender en los espacios de "comercio electrónico") que pueda despertar excitación sexual en alguna persona sexualmente interesada en niños, hasta fotos y videos de niños explotados de manera sexual y comercial ("pornografía infantil"), y espacios para contactar o comerciar el acceso a niños para su explotación. No es nuevo que redes de pedófilos se organicen en internet y por esa vía difundan fotografías, películas o imágenes generadas por computador, de menores en actos sexuales u obscenos, solos o acompañados. Ante esta violación a los derechos de los niños, se torna necesario tomar medidas de protección (legislación, policía cibernética, filtros) para que la red no sea un refugio impune a los pedófilos y explotadores de menores.

2. LA LEY REGULA LAS RELACIONES SOCIALES

En la sociedad, las relaciones sociales no son siempre armónicas, y por eso, establecemos leyes y regulaciones. La libertad no es absoluta ni ilimitada, y las personas tenemos derecho a la salud y a un ambiente sano: así lo disponen las leyes y los tratados vigentes en Costa Rica, donde la Constitución Política también es clara en señalar que "el Estado debe procurar el mayor bienestar de todos los habitantes del país". Ello implica que no puede permitir que se lesione a ningún grupo

[1] Miembro de la Comisión Nacional contra la explotación sexual comercial infantil de Costa Rica (CONACOES) desde 2002, en su calidad de asesora de la Diputada de la Asamblea Legislativa de la República de Costa Rica, Dra. Joyce Zurcher. Consultora en Salud Pública. Profesora de la Escuela de Medicina de la Universidad de Costa Rica. Email: yalenadelacruz@yahoo.com - delacruz@cariari.ucr.ac.cr Apdo. Postal 640-2050, San Pedro de Montes de Oca, San José, Costa Rica.

específico, y de manera particular, a los niños y adolescentes. Por eso, y porque "es evidente que la libertad no debe ser ilimitada a tal punto que entre en contradicción con los intereses singulares y de la colectividad"[2].

En cuanto a la libertad comercial, el análisis jurídico hecho en Costa Rica por la Sala Constitucional establece que implica la posibilidad de escoger una actividad para dedicarse a ella, pero no la posibilidad de incumplir la ley o menoscabar la dignidad de las personas o lesionar los valores de solidaridad y justicia de la colectividad: "la libertad de comercio consiste en la posibilidad de escoger libremente la actividad empresarial que mejor convenga al interesado, pero que una vez hecha tal escogencia, el respectivo tipo de actividad queda sujeto a todas las disposiciones que le sean aplicables. Si bien el cine y técnicas derivadas como la televisión y el video cine, son expresiones del comercio y de la industria, antes que de la libertad de opinión, su naturaleza de espectáculo público, los sitúa bajo la actividad administrativa que tiene por objeto la protección de la seguridad, la moralidad y la salubridad públicas. Es decir, bajo la potestad de regular el ejercicio de los derechos y el cumplimiento de los deberes constitucionales"[3]

3. EL CIBERESPACIO: NUEVA PLATAFORMA DE RELACIÓN SOCIAL

Las relaciones sociales han cambiado con la tecnología, pues han surgido nuevas plataformas para relacionarse, que incluyen: IRC (chats o "cuartos de conversación" virtuales), mensajes de voz, texto en y desde teléfonos celulares y computadoras, imágenes en internet y teléfonos, comercio electrónico, imagen y vídeo en computadoras y otros dispositivos de almacenamiento de datos (PDAs, Palms, cámaras digitales, etc).

Muchas de las interrelaciones en el ciberespacio son lícitas. No obstante, también internet es una plataforma para delinquir. Surgen así los llamados delitos cibernéticos que plantean, entre otros, un nuevo espacio para control policial y la categorización de los delitos informáticos.

4. LA EXPLOTACIÓN SEXUAL COMERCIAL INFANTIL EN INTERNET

Internet ha facilitado el contacto entre pedófilos, y entre estos y los menores a ser abusados; y ha permitido difundir la "erótica infantil", entendida esta como cualquier artículo que pueda despertar excitación sexual en alguna persona sexualmente interesada en niños (fotos, revistas, ropa íntima, etc). De ahí que se vuelva necesaria una policía cibernética y un grupo de medidas de protección, entre las que se incluyen filtros, regulaciones, rastreo de mensajes y medidas de cooperación internacional para hacer frente al desafío global de detener toda forma de explotación –sexual– de menores. Esto es particularmente importante para Costa Rica, que ha sido promovida como un "paraíso" para la pedofilia, la difusión de pornografía infantil y la explotación sexual comercial de menores, lo que ha sido evidenciado en diversos reportajes de la prensa costarricense e internacional. Además, "Costa Rica es un país con trata interna de personas y es primordialmente un destino de mujeres adultas y menores de edad para la explotación sexual"[4]

¿Qué hacer?

Sin perder el equilibrio entre seguridad pública y privacidad: es necesario hacer prevalecer el interés superior del niño, para lograr la "tolerancia cero" contra la pornografía infantil. Algunas acciones son: policía cibernética para el "patrullaje de la red", acciones preventivas, legislación para tipificar "delitos cibernéticos", cooperación internacional para el seguimiento de casos.

---

[2] Doctrina italiana. Citada por: Beirute, Farid. Acción de Inconstitucionalidad de Oscar Bákit. Procuraduría General de la República, p15, Costa Rica.

[3] Resolución de la Sala Constitucional Nº 611-91. 22 de marzo de 1991, Costa Rica.

[4] Trafficking in Persons Report. June 11, 2003. URL: http://www.state.gov/g/tip/rls/tiprpt/2003/21275.htm#costa rica

5. SENTIDO DE URGENCIA

Federico Mayor Zaragoza ha dicho[5] que nuestra única esperanza radica en la libertad y la creatividad humana para hacer frente a cuatro grandes desafíos:

• la construcción de la paz, con programas internacionales y cooperación planetaria (porque la mundialización de los acontecimientos debe suscitar la mundialización de las voluntades), no solo para evitar el horror de la guerra, sino sobretodo para preparar la justicia social y para desterrar la violencia

• la desaparición de las desigualdades y exclusiones, terriblemente agudizadas por la mundialización que ha fracturado la sociedad, y donde solo un quinto de la población del planeta se ha beneficiado en el proceso; el restante 80% ha sufrido las consecuencias en términos de trabajo, educación, salud, estructura familiar y pobreza, así como una rampante pérdida de valores --llamadas por Mayor, "enfermedades del alma"-- que ha hecho prevalecer "la ley de la jungla", la indiferencia y la pasividad, y desaparecer la solidaridad al tiempo que los gobiernos se preocupan solo por los asuntos económicos y no por las cuestiones sociales.

• el desarrollo duradero, que comprende el deber de prever para las generaciones futuras ("a las que, por egoísmo y miopía temporal, no podemos negarles sus derechos") y el fortalecimiento de la democracia para todos, donde prevalezca "la fuerza de la razón" y no "la razón de la fuerza", y donde todos podamos tener calidad de vida, que es educación, salud, trabajo y posibilidad de desarrollarnos plenamente en la sociedad.

• la visualización de un proyecto de largo plazo, para no ir a la deriva, porque "no hay viento favorable para quien no sabe a dónde va. No hay buen viento para un capitán que no puede descifrar un mapa", para quien no puede leer la realidad, y... hay que saber leerla en temas como el agua, la energía, el cambio climático planetario, la polución, la seguridad alimentaria, el desarrollo, el lavado de dinero sucio, el crimen organizado, la droga, las epidemias, los factores que degradan el ambiente, entre otros sugeridos por Mayor.

La cooperación internacional y las acciones nacionales contra la explotación sexual comercial infantil en internet se enmarca dentro de esos grandes desafíos para lograr un mundo de mayor justicia social, sin esa terrible forma de violencia y degradación que es la explotación sexual de menores; para buscar una sociedad inclusiva y participativa; para buscar un desarrollo armónico y con calidad de vida, y donde nuestro proyecto de largo plazo se sustente en una sociedad de oportunidades para los niños y no en su explotación.

6. ACCIONES EN COSTA RICA

Sin perder el equilibrio entre seguridad pública y privacidad, es necesario hacer prevalecer el interés superior del niño, para lograr la "tolerancia cero" contra la pornografía infantil, entendida en los términos de la ley de Hong Kong: cualquier fotografía, película, imagen generada por computadora u otra representación visual, de una persona que sea menor o aparente tener menos de 18 años; incluye imágenes generadas o hechas por cualquier medio, sean o no de una persona verdadera.

En ese sentido, es esperanzador el hecho de que el Ministerio de Seguridad Pública haya creado la "policía cibernética", y que el Gobierno de la República haya emitido una serie de decretos para controlar la explotación sexual comercial infantil, entre ellos, la regulación de los cibercafés y la gestión para que la Asamblea Legislativa ratifique la adhesión de nuestro país al Convenio del Consejo de Europa sobre la Ciberdelincuencia (23/11/01) y el Protocolo de Ciberxenofobia.[6]

6.1. Regulación de los locales que ofrecen servicio público de internet

Mediante decreto ejecutivo, y considerando el problema de salud pública que es la pornografía, así como lo establecido por la Convención Americana Sobre Derechos Humanos o Pacto de San José, aprobada por Ley No. 4534 de 23 de febrero de 1970, en su artículo 13.4) permite expresamente la

[5] Mayor Zaragoza, Federico. Un Mundo Nuevo. Ed. Odile Jacob, Paris, 1999

[6] Patronato Nacional de la Infancia (Presidencia Ejecutiva) , Ministerio de Seguridad Pública (Despacho de la Viceministra de Seguridad Pública), Asamblea Legislativa (Despacho de la Diputada Joyce Zürcher), Ministerio de la Presidencia. Compromiso y acciones contra la explotación de niños, niñas y adolescentes, San José, 2004.

censura previa de los espectáculos públicos con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia; y el mismo artículo 13, en su inciso 5, prohíbe la propaganda en favor de la guerra, toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, y las disposiciones de la legislación nacional específica sobre la materia, el Poder Ejecutivo emitió, en 2004, mediante decreto ejecutivo, el Reglamento de control y regulación de los locales que ofrecen servicio público de internet según el cual:

"Artículo 4. -Toda persona física o jurídica que solicite permiso sanitario de funcionamiento en un establecimiento de los indicados en el artículo 1 del presente decreto y desee que algunas de sus computadoras tengan acceso a pornografía, deberá adecuar una sección aislada del público en general, la cual no podrá exceder a más del 20% de la totalidad de las computadoras disponibles en el local, donde sólo tengan acceso mayores de edad y no esté permitido el ingreso de los menores de edad. Dicha sección deberá estar debidamente señalizada y para ingresar, el responsable o administrador del negocio deberá acreditar la mayoría de edad de los clientes."

"Artículo 5. -De Las Sanciones. La permanencia de una persona menor de edad en el área destinada exclusivamente para adultos, será causal para suspender temporalmente el permiso sanitario de funcionamiento al local en donde se preste el servicio de Internet. Dicha sanción se establecerá una vez que se compruebe la existencia de dicha falta, mediante la realización de un procedimiento administrativo en donde se observará y cumplirá con la garantía constitucional del Debido Proceso y los principios que la conforman. En caso que se demuestre por la misma vía procedimental, la reiteración de una falta igual, o se compruebe, aunque sea por primera vez, que, en forma dolosa, se perjudicó o quebrantó de algún modo, la integridad física, moral, sexual y/o mental de alguna persona menor de edad, se procederá conforme a la Ley 7899, sin perjuicio y con independencia de las demás sanciones que establezca el resto del ordenamiento jurídico."

"Articulo 7. El Ministerio de Salud establecerá un Certificado voluntario, para los cafés internet libres de pornografía, es decir, aquellos en los que la totalidad de las computadoras del local tienen filtros instalados para impedir el acceso a material pornográfico. Dicho Certificado se pondrá en lugar visible para todo el público. El Ministerio de Salud elaborará una lista por regiones de los cafés internet libres de pornografía, la cual estará disponible para todo el público."

El reglamento faculta a las autoridades del Ministerio de Seguridad Pública, del Ministerio de Salud y del Patronato Nacional de la Infancia, cada una en el ejercicio de sus propias competencias y en forma coordinada, para hacer cumplir el reglamento, y pide al El Patronato Nacional de la Infancia que propicie campañas educativas e informativas dirigidas a los padres de familia para que preferentemente sus hijos asistan a cafés internet certificados como "libres de pornografía".

6.2. Campaña de Seguridad Infantil en Internet en Costa Rica: Navegando sin Riesgo

El Patronato Nacional de la Infancia, en coordinación con Defensa de los Niños Internacional, (DNI-Costa Rica) desarrolla una campaña de seguridad en internet para prevenir formas de violencia sexual, con énfasis en pornografía, hacia los niños, niñas y adolescentes a través de la red internet.

Se busca así informar a los niños, niñas y adolescentes sobre los beneficios y riesgos de navegar en internet y darles algunas herramientas para su auto protección en escuelas y colegios e información sobre paginas educativas, que incluye el uso del filtro Optenet; a los padres, madres y responsables, sobre su responsabilidad de proteger a sus hijos e hijos de los riesgos de Internet, sus vínculos con la violencia sexual, y darles consejos sobre como protegerlos; a los educadores y funcionarios públicos, sobre de los mecanismos de denuncia penal existentes en el país, en relación a delitos sexuales contra la niñez y adolescencia; y a los Internet Café de los consejos sobre cómo navegar seguros en Internet.

6.3. Adhesión al Convenio del Consejo de Europa sobre la Ciberdelincuencia (Budapest, 23.XI.2001)

El Gobierno de la República ha solicitado al Ministro de Relaciones Exteriores y Culto que gire instrucciones a la misión costarricense en Ginebra, Suiza, para que analice los pasos y medidas a

tomar para que nuestro país se adhiera al Convenio del Consejo de Europa sobre la ciberdelincuencia y su protocolo sobre ciberxenofobia.

6.4. Creación de la Policía cibernética

El Ministerio de Seguridad Pública ha creado la Policía Cibernética, adscrita al Viceministerio de Seguridad Pública, para la investigación de casos vinculados con las áreas de trabajo de dicha instancia: propiedad intelectual y explotación sexual comercial de personas menores de edad.

CRIPTOANÁLISE EM JAVA

Antonio Marcos de Oliveira Candia[1]

Abstract

Cryptanalysis is an important tool in computer forensics. Various approaches have been used to implement high-performance computational cryptanalysis, however, they fail to provide an easy-to-use, portable and flexible solution. To achieve these goals we introduce the quebra-pedra framework. This framework provides dictionary and brute-force attacks and uses standard Java features to provide those requirements in a simple way and, at the same time, manages to achieve performance levels similar to those of C/C++ programming languages.

1. INTRODUÇÃO

A busca por evidências de atos criminosos na área forense computacional freqüentemente envolve a manipulação de informações que foram criptografadas. Quando não há cooperação no sentido de fornecimento da chave utilizada, deve se utilizar técnicas de criptoanálise para se extrair as informações originais. Uma das soluções é o uso de técnicas de criptoanálise computacional para realizar a busca pela chave utilizada para a geração do texto cifrado.

Dentre as várias técnicas de criptoanálise, conhecidas como ataques, algumas possuem cunho mais generalista, podendo ser empregadas em um maior número de situações. Os ataques considerados mais genéricos são, respectivamente, o ataque por força-bruta - ou varredura completa do espaço de chaves - e o ataque dirigido por dicionário. Estes ataques demandam grande custo computacional, pois baseiam-se no método de tentativa-e-erro. Portanto, para serem utilizados, requerem uma plataforma computacional de alto desempenho ou o resultado da busca não poderá ser conhecido em um espaço de tempo compatível com a realização de um inquérito criminal.

Outro ponto a ser levado em conta é o algoritmo utilizado para a encriptação dos dados. Atualmente existe uma enorme gama destes algoritmos, alguns de conhecimento público e amplamente documentados, outros de caráter proprietário e protegidos por patentes ou licenças restritivas de uso. Devido a esta variedade, a maioria dos sistemas de criptoanálise existentes engloba apenas uma parte destes algoritmos. Uma solução mais ampla é necessária.

Para possibilitar a realização de ataques criptoanalíticos desta forma, foi criado um arcabouço de programação (*framework*) denominado quebra-pedra. Este arcabouço foi projetado tendo como objetivos principais flexibilidade, portabilidade e desempenho. Este artigo mostra como a linguagem Java foi utilizada para alcançar tais objetivos.

2. CRIPTOANÁLISE COMPUTACIONAL

Várias ferramentas estão disponíveis hoje em dia para a realização de criptoanálise computacional. Dentre as mais conhecidas podemos citar sistemas como o L0phtCrack [1] e John The Ripper [2]. Estas ferramentas são capazes de realizar buscas por dicionário e/ou força-bruta, porém, normalmente sobre alguns tipos específicos de algoritmos criptográficos e, em sua maioria, são voltadas para a busca por senhas de acesso a sistemas. É possível extender estas ferramentas para qualquer algoritmo de criptografia, isto, entretanto, exige um grande esforço de programação, tornando-as inadequadas ao uso imediato com algoritmos criptográficos desconhecidos ou para os quais elas não estejam preparadas. Desta forma, surge a necessidade de uma ferramenta que não sofra estas restrições para o uso na área forense computacional.

[1]Laboratório de Sistemas de Computação, Curso de Ciência da Computação, Universidade Federal de Santa Maria. (LSC/CCC/UFSM)

O projeto desse tipo de sistema recai, primeiramente, sobre os tipos de ataques que o mesmo deve suportar. Vejamos, portanto, alguns detalhes sobre os ataques genéricos citados acima.

O ataque por força-bruta tem como característica principal a garantia de encontrar a chave criptográfica procurada, pois baseia-se em uma varredura total do espaço de chaves possíveis. Porém, como na maioria dos casos este espaço de busca possui um tamanho bastante grande, este ataque torna-se impraticável em um sistema convencional. Por exemplo, consideremos que o espaço de busca seja composto apenas pelo conjunto de caracteres formado pelos dez algarismos, pelas vinte e seis letras de nosso alfabeto e o caracter de espaço. Neste caso, se fôssemos testar todas as possíveis combinações de um a oito caracteres, chegaríamos ao número total de aproximadamente 361 trilhões de possibilidades . Assumindo-se que um sistema hipotético gaste um milésimo de segundo para testar cada possibilidade, teríamos um total de aproximadamente 1.002.778 horas ou 114,5 anos para cobrir todo este espaço de busca. Note-se que não foram incluídos neste cálculo os caracteres de pontuação, que corriqueiramente são utilizados para formação de chaves e que elevariam exponencialmente o número de possibilidades a serem testadas.

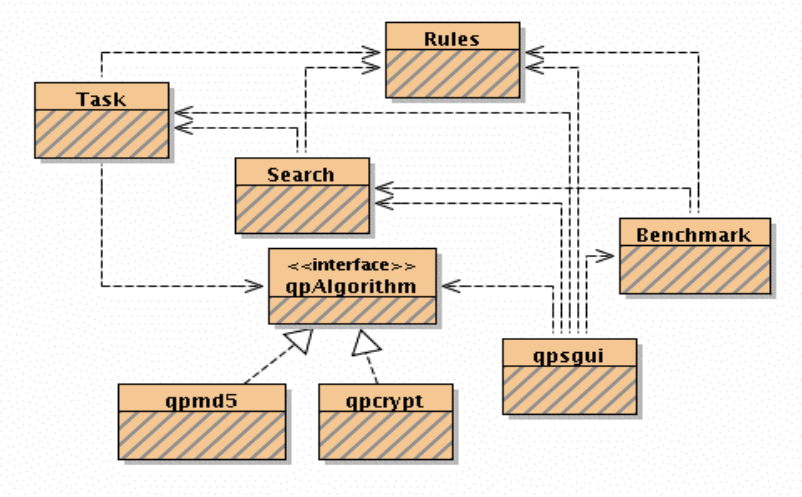
O ataque dirigido por dicionário é uma variação do ataque por força-bruta que busca diminuir este tempo total. Nesta modalidade de ataque o criptoanalista utiliza-se de um dicionário contendo palavras a serem testadas como chaves. Alguns sistemas implementam, além disso, a capacidade de utilização de um conjunto de regras de modificação que atuam sobre o dicionário básico, extendendo-o para englobar uma porção maior do espaço de busca total. Este tipo de ataque baseia-se na premissa de que uma grande porcentagem dos usuários escolhe suas chaves criptográficas dentre palavras presentes em seu vocabulário, ou modificações destas. Obviamente o sucesso deste ataque depende de a chave procurada estar presente no dicionário utilizado. Para aumentar esta probabilidade faz-se necessário o uso de dicionários adequados. Por exemplo, o dicionário da língua inglesa fornecido com as distribuições do sistema operacional Linux conta com aproximadamente 235.000 palavras. Utilizando os mesmos parâmetros do exemplo anterior, chegamos à conclusão que são necessários 4 minutos para testar todo o dicionário. O teste de cada modificação imaginada para este dicionário irá tomar os mesmos 4 minutos. Neste caso, cabe ao criptoanalista escolher aquelas modificações que aumentem a probabilidade de descoberta da chave, tendo em mente que cada uma será testada de forma relativamente rápida.

Para permitir um mecanismo simplificado de criptoanálise, tornou-se necessário, portanto, o projeto e implementação de uma ferramenta extensível, portável, de alto desempenho e baixo custo. Estas são as premissas básicas do arcabouço quebra-pedra.

3. QUEBRA-PEDRA: UM ARCABOUÇO GENÉRICO PARA CRIPTOANÁLISE

Quebra-pedra (qp) é um arcabouço Java genérico para criptoanálise baseada em varredura de espaço de soluções. Mais especificamente, este sistema oferece as técnicas de ataque por força-bruta e busca dirigida por dicionário e dá ao criptoanalista a capacidade de extender o seu uso a qualquer problema de criptoanálise que possa ser atacado pelas técnicas oferecidas. Atualmente, a plataforma conta com uma implementação seqüencial (*stand-alone*) capaz de realizar estes ataques e que demonstra o potencial deste arcabouço, denominada *qpseq*. A figura 1 mostra a arquitetura básica desta implementação.

Figura 2: Diagrama de classes de uma aplicação seqüencial de busca de chaves utilizando o arcabouço quebra-pedra



O arcabouço foi projetado em torno dos seguintes princípios:
independência de plataforma de execução (compatibilidade/interoperabilidade);
independência de algoritmos de criptografia (extensibilidade);

A independência de plataforma de execução é importante pois permite ao usuário utilizar-se de qualquer processador de propósito geral para a realização das buscas. Esta independência permite ao criptoanalista escolher qual processador melhor se adapta à tarefa a ser realizada. Para se conseguir esta independência, optou-se pelo uso da linguagem de programação Java para a implementação do arcabouço. Esta linguagem permite, atualmente, a utilização do mesmo código em uma grande gama de processadores, mostrando-se uma alternativa adequada aos requisitos de interoperabilidade do sistema.

Quanto à independência de algoritmos de criptografia, ainda no estágio inicial de projeto tornou-se claro que esta seria uma característica chave do sistema. Como exposto anteriormente, os sistemas atuais não são facilmente adaptáveis a algoritmos diferentes daqueles para os quais foram projetados. Isto cria uma situação em que sua praticidade de uso torna-se baixa, pois em computação forense, constantemente são necessárias buscas que envolvem novos métodos criptográficos. Ou seja, se a plataforma criptoanalítica não for adaptável, tornaria-se obsoleta rapidamente. Este problema foi resolvido, no quebra-pedra, com o uso de conceitos disponibilizados pela linguagem Java.

O sistema conta com um mecanismo simples, porém flexível de adaptação para uso geral. Este mecanismo baseia-se em dois conceitos introduzidos na plataforma Java a partir da versão 1.3: o código reflexivo e a interface nativa Java. [5]

A Reflexão é um conceito que permite, dentre outras coisas, a carga dinâmica de código em tempo de execução. Isto permite a modificação de um sistema para a adição de funcionalidade sem a necessidade de uma nova compilação do mesmo. Já a interface nativa Java (*Java Native Interface* - JNI) permite o uso de código nativo escrito em linguagem C/C++ que esteja na forma de DLL (em ambiente *Microsoft Windows*) ou de biblioteca de carga dinâmica .so (em ambiente *Unix*).

O uso destes conceitos em conjunto permite, portanto, a carga dinâmica de código nativo sem a necessidade de recompilação do sistema de criptoanálise. Para enterdermos como este mecanismo funciona, vejamos um exemplo: uma situação em que um criptoanalista depara-se com um conjunto de dados criptografados e, após uma análise inicial, chega à conclusão que foi utilizado um programa proprietário para esta criptografia. Analisando este programa, ele descobre que o mesmo utiliza um algoritmo criptográfico desconhecido. Nesta situação o analista pode se utilizar das bibliotecas usadas pelo programa original para a busca da chave no quebra-pedra. Para isto, é necessário realizar a programação de um pequeno adaptador extremamente simples para o quebra-pedra e o sistema estará apto a auxiliá-lo em sua tarefa. Este modelo de reuso de código nativo elimina, portanto, a tarefa de

reprogramação ou mesmo recompilação do quebra-pedra como um todo para seu uso com novos algoritmos de criptografia tornando-o totalmente adaptável de forma simples e rápida.

O adaptador é uma pequena classe Java que deve implementar uma interface específica (*qpAlgorithm* na figura 1). Um criptoanalista que pretende utilizar o quebra-pedra com um algoritmo ainda não disponível no mesmo precisa somente programar este pequeno adaptador. Alguns exemplos são fornecidos com o sistema para tornar esta tarefa ainda mais simples. Novamente na figura 1 podemos notar a presença de dois destes adaptadores: *qpcrypt* e *qpmd5*.

Como vantagem adicional, este método isola o criptoanalista de detalhes de implementação da plataforma, tais como protocolos de comunicação, mecanismos de distribuição,etc. Além disso, outra vantagem importante é o fato de que o método de verificação é desacoplado do arcabouço, pois fica no adaptador. Isto significa que o analista pode utilizar o sistema para tarefas simples como a quebra de senhas ou tarefas mais complexas, como a busca por chaves utilizadas para a criptografia de textos, arquivos compactados, fragmentos de arquivos e assim por diante.

Outras características do disponibilizadas pelo arcabouço são: salvamento automático do estado da execução, cache de sucessos e reconhecimento de texto. A primeira quer dizer que o sistema salva automaticamente um ponto de referência (*checkpoint*) do estado de execução. Se por alguma razão o sistema for parado antes de ocorrer uma quebra ou chegar ao fim da busca, na próxima execução a busca será reiniciada deste ponto de referência. Quanto à cache de sucessos, o sistema possui um mecanismo que guarda automaticamente todas as chaves encontradas. Esta cache sempre é verificada antes de se iniciar qualquer busca, evitando assim o desperdício de recursos com repetição de trabalho já feito. Finalmente, o arcabouço conta com uma classe que possibilita o reconhecimento de texto a partir de análise estatística. Esta classe implementa a equação de Sinkov, conhecida como logaritmo da verossimilhança (*log-likelihood*) [8], além de métodos para o cálculo e armazenamento de tabelas de freqüência utilizadas por esta equação. Desta forma, um criptoanalista pode usá-la no adaptador para realizar buscas dirigidas à uma linguagem ou padrão específico de texto.

4. DESEMPENHO DO SISTEMA

A linguagem Java é frequentemente citada como tendo baixo desempenho, porém, poucos estudos realmente a avaliaram neste aspecto e nenhum na área de criptoanálise. Para verificar a viabilidade do arcabouço, portanto, foram feitas análises de desempenho do *qpseq*. Estas análises basearam-se na execução de buscas simples utilizando os métodos de dicionário e força-bruta com o algoritmo DES e levaram aos seguintes resultados:

Implementação	**Tempo em relação à C**
Java com Hotspot	~8
Java com JNI	~1,15

Tabela 1: Comparação de tempos de execução entre qpseq e uma implementação em linguagem C

Ou seja, para o algoritmo citado, a implementação interpretada que utiliza a plataforma Hotspot para execução do código Java foi cerca de 8 vezes mais lenta que a implementação de referência e a versão que utiliza chamadas à código nativo através da JNI foi cerca de 1,15 vezes mais lenta somente. Resultados preliminares com outros algoritmos demonstram esta mesma tendência em favor da implementação com JNI. Em ambos os casos a plataforma Java utilizada foi a Sun JRE versão 1.4.2 em um computador Pentium IV 2.4GHz rodando o sistema operacional Linux, *kernel* versão 2.4.22..

Destes testes conclui-se que a linguagem Java interpretada realmente é lenta para o fim específico de criptoanálise, mas em conjunto com o mecanismo de execução de código nativo JNI torna-se uma alternativa bastante atrativa. Se levarmos em conta outras características inerente à Java como simplicidade de programação e a capacidade de carga dinâmica de código através da reflexão, a sobrecarga citada acima torna-se irrelevante.

5. OBTENDO DESEMPENHO SUPERIOR: PROCESSAMENTO PARALELO

Observações simples mostram que um computador pessoal típico é sub-utilizado pois fica a maior parte do tempo em estado ocioso e, portanto, poderia ser utilizado para resolver problemas que necessitem de grandes recursos computacionais. Estes processadores ociosos podem ser utilizados para a execução concorrente de tarefas. Alguns exemplos conhecidos de sistemas que utilizam esta abordagem de "compartilhamento de ciclos ociosos de UCP" são o SETI@Home [3] e suas variantes [4]. Esta arquitetura de processamento concorrente é chamada, atualmente, de Computação Colaborativa por permitir que usuários - ou seus processadores mais especificamente - trabalhem juntos para alcançar a solução de um problema. [1,4]

A programação da versão distribuída do quebra-pedra está sendo realizada através da biblioteca ProActive. Essa biblioteca faz parte do projeto ObjectWeb Middleware, uma comunidade de desenvolvimento no modelo *open-source* que atualmente possui sua sede no INRIA, instituto nacional francês de pesquisa em ciência da computação [6]. Resultados preliminares mostram que o ganho de desempenho é significativo. Maiores estudos são necessários, entretanto, para quantificar este aumento.

6. CONCLUSÕES

O uso da linguagem Java para a programação de sistemas de criptoanálise, a despeito dos problemas de desempenho da linguagem, fornece uma solução de alto-desempenho, portabilidade extensibilidade e facilidade de uso. Conceitos introduzidos à linguagem permitem estas características, em especial o código reflexivo e a interface nativa Java. Com base nestas considerações, este artigo mostrou o arcabouço quebra-pedra que oferece um conjunto mínimo de ferramentas para simplificar a criação dessas aplicações.

7. REFERÊNCIAS BIBLIOGRÁFICAS

[1] Roy D Williams et. al., "Parallel Computing Works", Morgan Kauffman Publishers, 1994.
[2] Anderson, David P. et al., "SETI@home: an experiment in public**-resource computing,** *Communications of the ACM*, 45(11), pp56-61, Novembro de 2002.
[3] A. Grimshaw, et al.,"Wide-Area Computing: Resource Sharing on a large scale", IEEE Computer, pp1-9, Maio de 1999.
[4] R.K. Joshi and D. J. Ram, "Anonymous Remote Computing: A paradigm for parallel programming on interconected workstations", IEEE Trans on software engineering, Vol 25, No 1, pp75-90, Janeiro de 1999.
[5] Sun Microsystems, "Java 2 SDK Standard Edition Documentation", disponível em http://www.java.sun.com/, acesso em Maio de 2004.
[6] D. Caromel, W. Klauser, J. Vayssiere, "Towards Seamless Computing and Metacomputing in Java", Concurrency Practice and Experience, 10(11-13), pp. 1043-1061, Setembro de 1998.
[7] Seeley, Donn. "Password cracking: a game of wits", Communications of the ACM, 32(6), pp700-703, Junho de 1989.
[8] Ganesan, R.; Sherman, A. "Statistical Techniques for Language Recognition: An Introduction and Guide for Cryptanalysts", Cryptologia, 17(4), pp321-366, Fevereiro de 1993.

"LUPA DIGITAL", UMA FERRAMENTA PARA OTIMIZAÇÃO DE BUSCA DE IMPRESSÕES DIGITAIS

Marcelo Garrido de Oliveira
UnB – Universidade de Brasília, Brasília - DF, Brasil, marcelo.garrido@bcb.gov.br

Marcelo Ladeira
UnB – Universidade de Brasília, Brasília - DF, Brasil, mladeira@cic.unb.br

Marcos Elias Cláudio de Araújo
Instituto Nacional de Identificação do DPF, Brasília – DF, Brasil
marcos.meca@bol.com.br

Abstract

Brazil's Federal Police Identification Institute, DPF/INI, has applied biometrical skills in identification process of people involved in crime. This article is based on DPF/INI data, and it searched to deepen the study of application of data mining skills in this domain. DPF/INI files are based on manual search, with fingerprint classify system proposed by Vucetich, considered that the relative codes of ten fingerprints of a person are available. However, in the scene of crime, they only fragments of fingerprints are found. The goal is obtain a classifier model that generate Vucetich codes for the fingerprints of the missing fingers permits reduce the space of search in manual or automatic searching for fingerprints identification. "Lupa Digital" is a consult tool developed in Java, which revealed capable to reduce the effort of search in consults and also produce probabilistic information about some physical characteristics related with Vucetich fingerprints codes evidences.

1. INTRODUÇÃO

Fundamentado em informações de impressões digitais e outros atributos físicos o presente artigo, iniciou-se com a extração, preparação e análise de um banco de dados com 502.052 registros, denominado de MECA-Sinic, assim como no estudo de mineração de dados sobre o arquivo datiloscópico criminal do Instituto Nacional de Identificação, vislumbra e constata um enorme conjunto de possibilidades, entre elas a solução de crimes de forma mais eficaz e a melhoria da eficiência policial. Seu estudo aprofundado pode respaldar critérios técnicos na elaboração de suporte aos procedimentos periciais e aos sistemas informatizados de pesquisa de impressões digitais (AFIS – Automated Fingerprint Identification System), além de fornecer subsídios para estudos nos campos de outras ciências. Seus desdobramentos são, como a própria Criminalística, multifacetados, com repercussão em si mesma e em outras áreas do conhecimento humano.

2. O PROCESSO DE IDENTIFICAÇÃO DATILOSCÓPICA

Para que possamos diferenciar uma pessoa da outra é necessário que haja um método destinado a estabelecer sua identidade, ou seja, determinar um conjunto de caracteres próprios que possam individualizar pessoas ou coisas entre si. Afinal, mais do que identificar pessoas, precisa-se individualizá-las.

A biometria, ciência criada por Francis Galton[1] e Karl Pearson[2], é o ramo da ciência que estuda as medidas físicas dos seres vivos, daí o termo identificação biométrica para indicar as tecnologias que permitem a identificação das pessoas através dos traços físicos característicos e únicos de cada ser humano: os traços faciais, a íris, a retina, a voz, a grafia e a impressão digital.

Historicamente dentre os vários métodos já utilizados o Papiloscópico resultou como sendo o mais eficaz, por conseguir individualizar as pessoas tanto civil, quanto criminalmente [2]. A papiloscopia (papilla=papila e scopêin=examinar) é a ciência que trata da identificação humana através das papilas dérmicas, e que tem exercido seu papel de relevância no âmbito da pesquisa criminológica. Como ciência detém seus princípios: perenidade, imutabilidade e variabilidade dos desenhos papilares. Seu campo de atuação divide-se em Datiloscopia (dactilo=dedos), Quiroscopia (quiro=mãos) e Podoscopia (podo=pés).

Juan Vucetich[3] (1858-1925) foi um dos criadores do primeiro sistema de identificação humana com base em impressões digitais. Ele dividiu as impressões digitais em 4 tipos fundamentais: Arco (1); Presilha Interna (2); Presilha Externa (3) e Verticilo (4). Atualmente foram acrescentados mais 3 tipos, o Anômalo (5), a Cicatriz (6) e Amputação (7).

O Processo Papiloscópico foi introduzido no Brasil em 05 de fevereiro de 1903 e posteriormente coube ao Instituto Nacional de Identificação - INI, órgão do Departamento de Polícia Federal, fundado em 1963, com sede em Brasília, a tarefa de centralizar todas as informações criminais no Brasil, agregado aos dados antropológicos, como forma de individualização dos delinqüentes.

3. A APLICAÇÃO "LUPA DIGITAL"

A termo "**Lupa Digital**", representa uma ligação entre uma das principais ferramentas de trabalho no domínio da datiloscopia, a lupa, e o termo "digital" de duplo sentido neste caso, que associa tanto os dedos quanto o significado digital empregado na computação.

A linguagem JAVA foi escolhida devido à sua independência de plataforma (portabilidade), além de seguir o paradigma de orientação a objetos, o que facilita a inserção de novos recursos, a sua manutenção, reutilização de código e internacionalização.

3.1. Modelagem de Classes

A linguagem de representação escolhida foi a UML ("*Unified Modeling Language*"). O **Lupa Digital** foi dividido em quatro pacotes, são eles:

Pacote *default:* possui a classe "***Main***", responsável pelo início da aplicação **Lupa Digital**. Sua única atribuição é invocar a classe *Controlador* do pacote ***AIM***.

Pacote *AIM*: Pacote ilustrado pelo diagrama de classes da Figura 3.1. Este pacote possui as principais classes da aplicação **Lupa Digital** que implementam as telas de consulta e as classes de pesquisa decadactilar.

[1] Francis Galton, antropólogo, meteorologista, matemático e estatístico, nasceu em 16 de fevereiro de 1822, Birmingham no Reino Unido. Foi o criador dos termos Finger Prints (Impressão digital), Biometria e Eugenia, [1]

[2] Karl Pearson (1857-1936) era um matemático inglês, um dos fundadores da moderna estatística. Aplicou seus métodos de estatística a problemas biológicos de hereditariedade e evolução, dando assim contribuições matemáticas à teoria da evolução. Fonte: ©Encyclopaedia Britannica do Brasil Publicações Ltda.

[3] Juan Vucetich Kovacevich (1858-1925), é iugoslavo naturalizado argentino.

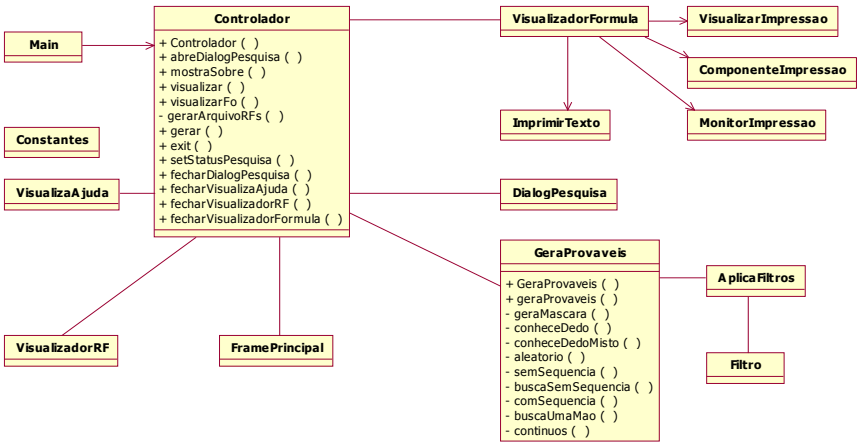


Figura 3.1 – Diagrama de Classes da aplicação *Lupa Digital*

Pacote *AIM.estruturas:* Possui as classes que especificam as principais estruturas de dados a serem utilizadas na pesquisa decadactilar.

Pacote *AIM.util:* Possui as classes que se encarregam da impressão da lista de fórmulas para orientar a pesquisa manual no arquivo AID.

3.2. Principais estruturas de dados

FreqForm: composta pelas fórmulas extraídas da base *FreqForm.dat*, suas respectivas freqüências de classe (contador).

Dedos: composta pelos principais atributos extraídos da base *MECA-Sinic.dat*;

Provaveis: composta pelas fórmulas extraídas da estrutura *FreqForm* e suas respectivas freqüências de classe (contador).

3.3. Operação do Lupa Digital

O **Lupa Digital** é iniciado com a execução do arquivo ***Lupa.jar***, apresentando a tela inicial conforme Figura 3.2.

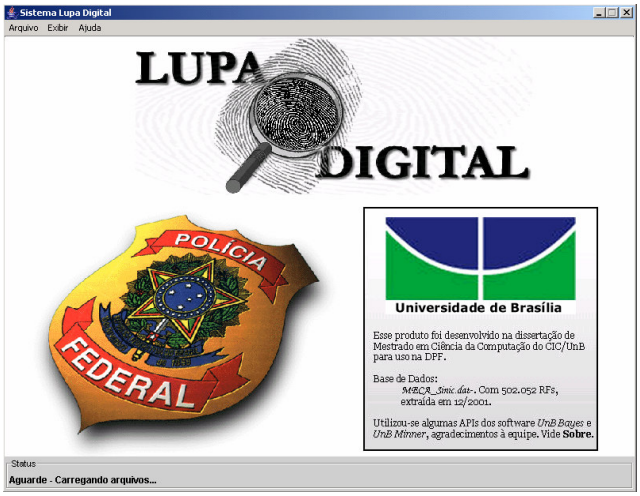


Figura 3.2 – Tela Inicial do Lupa Digital

A opção de menu "Arquivo > Pesquisa" gera a tela de pesquisa decadactilar que divide-se em quatro painéis, ilustrado na Figura 3.3:

- seleção da pesquisa: em verde. Define o tipo de pesquisa;
- painel de digitação dos dedos e filtros: em vermelho;

- painel de botões: em azul. Estes serão representados neste artigo pelo identificador dos mesmos, delimitado por colchetes, ex: [**Filtros**];
- painel de status: delimitado na Figura 3.3 pelo tom amarelo.

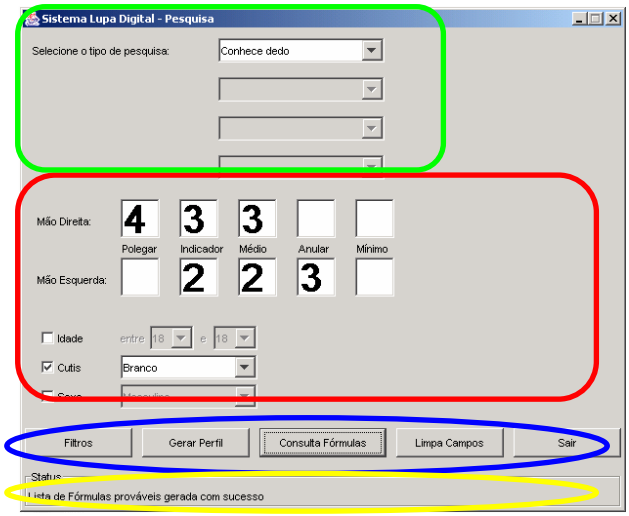


Figura 3.3 – Tela de Pesquisa do Lupa Digital

O uso de filtros é acionado pelo botão [**Filtros**] que habilita a área de opções de filtros no painel de digitação, conforme Figura 3.3. O uso dos filtros é admitido em qualquer tipo de consulta, aumentando a evidencia informada.

Pesquisa "Conhece Dedo"

Utilizada caso o especialista conheça a exata posição, nos dedos das mãos, das impressões digitais coletadas.

Pesquisa "Não Conhece Dedo"

Utilizada caso o especialista não conheça a exata posição, nos dedos das mãos, das impressões digitais coletadas. Deve-se escolher a opção de pesquisa que pode ser "Aleatório", o *default*, ou "Dedos da mesma mão".

Aleatório: Deve-se digitar em qualquer ordem os tipos primários coletados nos campos sem identificação de dedos. A pesquisa, neste caso, é feita variando-se todas as possibilidades nas duas mãos.

Dedos da mesma mão: Se a opção escolhida for "Dedos da mesma mão" então deve-se definir os valores de outros dois "Combo box", são eles:

conhece a ordem dos dedos: tem-se como opção: sim, não ou contínuos;

Selecione a mão: neste campo, deve-se definir a mão alvo da pesquisa, com as opções: mão direita, mão esquerda e ambas as mãos.

Pesquisa "Misto"

Utilizada caso o especialista conheça a exata posição, de alguns dedos das mãos, das impressões digitais coletadas, e, ao mesmo tempo, desconheça a posição de outras impressões coletadas.

Saídas

O **Lupa Digital** produz três tipos de saídas: telas de visualização, impressão e arquivo de RFs.

Tela de Visualização de Fórmulas

Acionada após os algoritmos de pesquisa gerarem a lista de fórmulas que atendem o critério da pesquisa. Suponha que uma pesquisa cuja posição dos dedos é conhecida foi acionada, conforme ilustra a Figura 3.3.

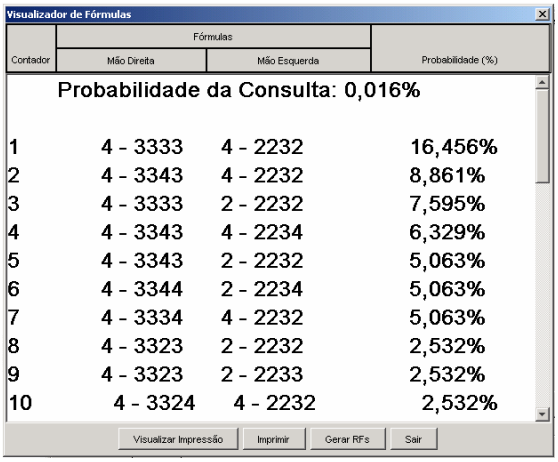


Figura 3.4– Tela Visualizador de Fórmulas

A primeira linha da área de rolagem do visualizador, Figura 3.4, define o percentual da base MECA-Sinic que atende ao critério de pesquisa, as evidências, especificado na Figura 3.3.

A primeira coluna de todas as linhas corresponde a um contador de Fórmulas que servirá para auxiliar na divisão da tarefa de pesquisa no arquivo AID, manual. A segunda e terceira colunas correspondem às fórmulas que atenderam ao critério de pesquisa. A última coluna define a probabilidade condicional de uma determinada fórmula dado o critério de pesquisa. No exemplo da Figura 3.4 tem-se que a fórmula 4-3333/4-2232 possui a probabilidade 16,456%, que significa: "dado o sub-conjunto de 0,016% do universo de pesquisa, a probabilidade da fórmula 4-3333/2-2232 corresponder aos dedos coletados é de 16,456%".

Os botões na parte inferior acionam o visualizador de impressão, a rotina de impressão e o visualizador de RFs, que serão detalhados a seguir.

Tela de Visualização de RFs

O visualizador de RFs apresenta a fórmula datiloscópica que agrega um grupo de RFs nas duas primeiras linhas do bloco, juntamente com a probabilidade condicional da fórmula. As demais linhas do bloco são mostram as RFs associadas àquela fórmula.

Janela de impressão

Acionada pelo botão [**Imprimir**] do visualizador de fórmulas. Nela o especialista definirá a impressora que receberá o job de impressão.

Tela de Visualização de impressão

Acionada pelo botão [**Visualizar Impressão**] do visualizador de fórmulas, nele pode-se fazer um ajuste da página. Através dele o especialista pode fazer ajustes na página de impressão antes de executá-la.

4. CONCLUSÃO

Destacam-se os aspectos quantitativos como a redução de tempo em uma pesquisa na base manual, o tempo de resposta da ferramenta e o "ganho" proporcionado pela mesma. Já os aspectos qualitativos referem-se à facilidade de uso da ferramenta e a obtenção de resultados antes impossíveis devido à complexidade do tipo de consulta.

Escolheu-se como ponto de partida para avaliação a situação mais simples de pesquisa que é inferir um dedo a partir da evidência dos outros nove. Para se calcular o ganho proporcionado pela ferramenta foi gerada uma planilha que quantificava o tempo gasto para pesquisar um determinado

tipo primário (ex: arco) em certo dedo da mão. Esta quantidade é chamada genericamente nesta pesquisa de "unidade de tempo" – UT, pois o tempo gasto por um datiloscopista para uma determinada pesquisa pode ser diferente do tempo gasto por outro datiloscopista para a mesma pesquisa. Desta forma, fez-se necessário a normalização destas unidades de tempo em uma única, a UT, para fins comparativos.

A tabela gerada relaciona os dez dedos da mão com os sete tipos primários, nas células acumula-se o valor das UTs. As duas últimas linhas dessa tabela referem-se a dois percentuais de ganho de tempo para uma pesquisa realizada para a fórmula em destaque. Foram escolhidas duas fórmulas para se avaliar o ganho. A Tabela 4.1 refere-se à avaliação da fórmula:

$$\frac{\mathbf{4-4444}}{\mathbf{4-4444}}$$

Tabela 4.1 - Cálculo de Unidades de Tempo (UT) para a fórmula 4-4444/4-4444

	DEDOS									
TIPOS	PD	ID	MD	AD	ND	PE	IE	ME	AE	NE
1	4	6	10	1	13	19	7	0		0
2	15	63	54	2	3	52	22	32	204	12
3	64	76	128	65	4	84	80	19	0	0
4	51	86	100	80	159	234	117	55	169	170
5	6	1	1	0	0	16	0	0	0	0
6	6	74	96	21	93	34	73	73	21	120
7	14	37	23	15	18	23	26	26	21	24
TOTAL	160	343	412	184	290	462	325	205	415	326
Ganho	61,94%	62,77%	65,75%	45,95%	11,17%	39,85%	48,23%	48,11%	54,69%	6,59%

O procedimento manual de busca no AID sempre começa da hipótese do tipo primário 1 e vai até o tipo 7, pois assim está organizado o AID. Neste caso, o resultado correto será sempre 4, ou seja, a busca pára neste valor. Chamou-se o percentual acumulado até o ponto de parada de "Ganho". A média do "Ganho" de tempo é de 44,51% para a fórmula acima.

A Tabela 4.2 documenta a avaliação de outra fórmula, composta de outros tipos primários, justificando a diferença de "Ganho" de tempo.

$$\frac{\mathbf{3-3333}}{\mathbf{2-2222}}$$

Tabela 4.2 - Cálculo de Unidades de Tempo (UT) para a fórmula 3-3333/2-2222

	DEDOS									
TIPOS	PD	ID	MD	AD	ND	PE	IE	ME	AE	NE
1	26	15	13	4	9	24	11	25	13	13
2	29	141	132	14	91	73	110	3	81	36
3	519	208	111	120	76	56	133	71	98	56
4	2922	173	112	163	63	200	94	7	71	153
5	25	35	0	9	4	0	52	2	7	4
6	193	25	15	141	8	5	25	11	10	8
7	20	0	40	30	35	23	88	1	33	37
TOTAL	3734	597	423	481	286	381	513	120	313	307
Ganho	9,58%	42,86%	56,64%	13,04%	56,82%	24,74%	9,09%	89,29%	13,83%	26,53%

Pela Tabela 4.2 percebe-se que com os tipos primários de menor ordem o "Ganho" médio de tempo também diminui (34,24%). Percebeu-se também que o ganho de tempo depende tanto do dedo como do tipo primário. Porém, independente da afirmativa anterior, sempre haverá maior ganho de tempo quanto maior for o número do tipo primário, pois esta é uma premissa da busca manual.

Quanto à hipótese de se fazer a mesma simulação supondo a ausência de dois ou mais dedos pode-se afirmar ser de grande dificuldade a impossível. Ela torna-se difícil quando a quantidade de dedos em dúvida é baixa e impossível quando passar de cinco dedos. Manualmente esta tarefa é irrealizável, devido ao grande número de possibilidades. Entretanto, pode-se afirmar que sempre o ganho de tempo será maior quanto maior for a ausência dos dedos.

Quanto ao ganho proporcionado pelo **Lupa Digital** nas pesquisas de dedos não posicionais como: aleatório, contínuos, dedos da mesma mão (com ordem conhecida, sem ordem conhecida), pode-se afirmar que tratava-se de uma tarefa antes irrealizável. Além de se tornar realizável o **Lupa Digital** proporcionou um método de busca manual orientada focando apenas as fórmulas que atendem os critérios de pesquisa definidos na consulta.

A ferramenta **Lupa Digital** atendeu às expectativas do DPF/INI otimizando as pesquisas realizadas com a evidência de sete ou mais dedos, viabilizando as pesquisas com número inferior de dedos como evidência e possibilitando as pesquisas sem conhecimento de posição dos dedos,

impraticáveis anteriormente. Seu desenvolvimento requereu o desenvolvimento de algoritmo específico para pesquisa decadactilar, pois não dá para se definir "*a priori*" a seleção das regras, visto que a inferência é feita de acordo com a consulta definida "*on-line*".

Adicionalmente, ela provê um meio de otimizar a pesquisa com o uso de uma solução AFIS, adquirida recentemente pela DPF, pois o arquivo com a lista de RFs gerada reduz em muito o universo de busca, ao mesmo tempo que orienta a ordem de pesquisa neste.

A aplicabilidade da ferramenta **Lupa Digital** extrapola o âmbito do DPF/INI, podendo ser utilizada em outros serviços de segurança pública, bastando para a isso, obviamente, o preparo dos arquivos de entrada para enriquecer a base existente com dados locais.

5. REFERÊNCIAS BIBLIOGRÁFICAS

[1] Barberá, Francisco Antón & Turégano, Juan Vicente de Luis y. "Policía Científica – Volume I". 3ª. Edição, Espanha, 1988. Página 78.

[2] *Identificação Papiloscópica*, Brasília - DF. Instituto Nacional de Identificação – DPF, uso interno, 1987. Ed. Serviço Gráfico do DPF.

[3] *Cross Industry Standard Process for Data Mining*. Disponível por WWW no site do padrão CRISP-DM – www.CRISP-DM.org.

[4] HAYKIN, Simon. *Redes neurais: princípios e prática.* Bookman, 2.ed., trad. Paulo Martins Engel, 2001.

[5] LADEIRA, M., VICCARI, R.M., COELHO, H. *Raciocínio Probabilístico em Sistemas Inteligentes.* In: CONGRESSO DA SOCIEDADE BRASILEIRA DE COMPUTAÇÃO, 19.; Jornada de atualização em informática, JAI, 18., 1999, Rio de Janeiro. Anais. Entre Lugar. v.2, p.307-365.

[6] SPIEGEL, Munrray R. Estatística. Tradução e revisão técnica Pedro Consentino – 3ª ed. – SP : Makron Books (Coleção Schaum), 1993.

COMBATENDO CRIMES CIBERNÉTICOS - PROTEÇÃO JURÍDICA NO BRASIL

André Machado Caricatti

Instituto Nacional de Tecnologia da Informação - CC/PR
Brasília - DF - BRASIL
andrecaricatti@apcf.org.br

Jorilson da Silva Rodrigues

Coordenação-Geral de Tecnologia da Informação - MJ
Brasília - DF - BRASIL
jorilson@apcf.org.br

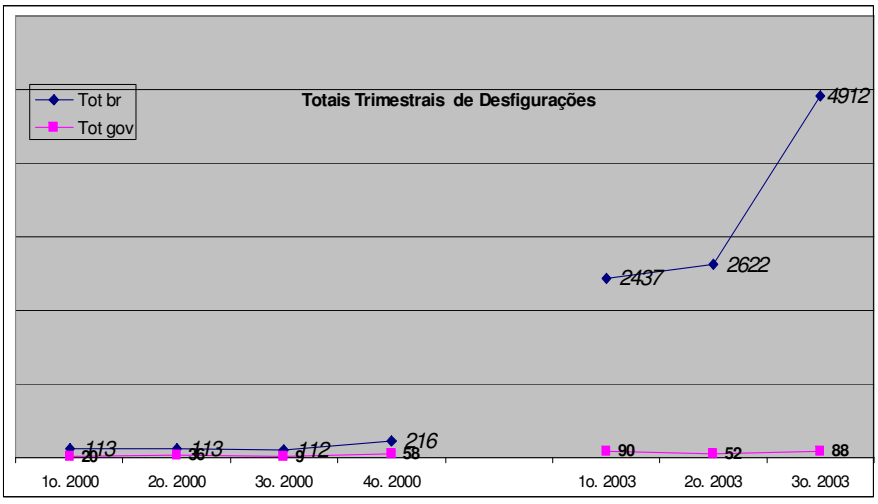
Resumo

A inserção da tecnologia da informação em atividades delituosas reflete avanços e melhorias que aquela apresenta. A proteção que o Poder Público oferece contra tais ameaças se torna eficaz ao combinar medidas cabíveis com agentes públicos devidamente capacitados, desde que haja a condição primeira da existência de leis provendo o resguardo dos bens jurídicos. Este artigo apresenta o momento do Direito no Brasil com uma visão estruturada, comparando os estatutos disponíveis com o modelo de referência internacional de maior aceitação, a Convenção sobre Crimes Cibernéticos do Conselho da Europa - ETS 185.

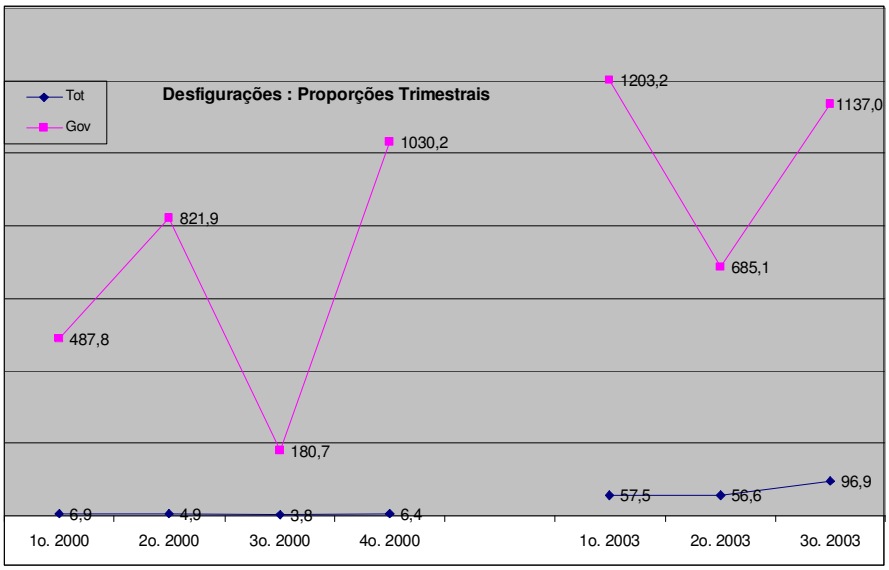
1. O BRASIL NO MOMENTO PRESENTE

A observação dos incidentes de segurança no domínio ".br", a parcela brasileira da Internet, traz dados relevantes. O número de incidentes reportados tem crescido consistentemente nos últimos anos.

Consolidando informações provenientes de Centros de Tratamento de Incidentes nacionais, como o Centro mantido pelo Comitê Gestor da Internet no Brasil – NBSO – e aquele que trabalha com a comunidade acadêmica - CAIS/RNP. Observa-se claramente que um número crescente de domínios nos diversos segmentos da Internet no Brasil tem sido alvo de ataques constantes e cada vez mais sofisticados.

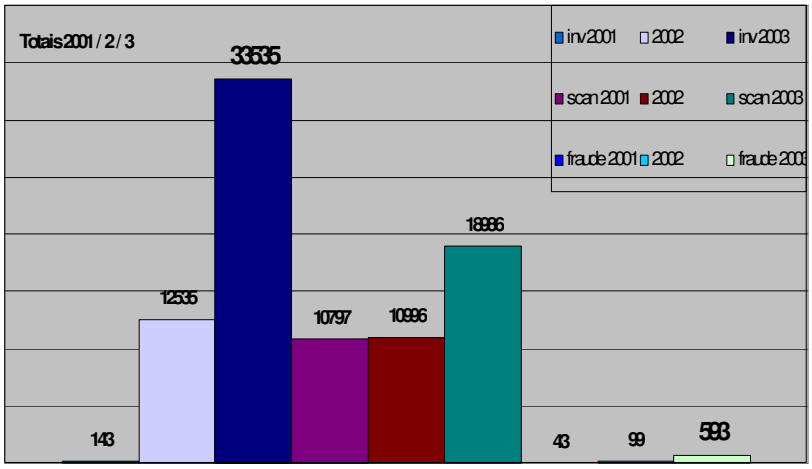


Quadro 1 – Números absolutos de desfigurações (defacements) em sítios da Internet brasileira (Tot), separados os governamentais (Gov). Dados consolidados nos trimestres de 2000 e 2003.



Quadro 2 - Proporção de desfigurações considerando o total geral de sítios (Tot) e parcela governamental (Gov). Fórmula : (Total de incidentes da categoria/ Total de domínios da categoria) * 10.000.

Embora o número absoluto de incidentes possa parecer reduzido para domínios governamentais, a exemplo de 52 desfigurações no 2º. trimestre de 2003, proporcionalmente ao total de 759 sítios ".gov.br" a relevância torna-se outra [1].



Quadro 3 – Totais de incidentes reportados nos anos de 2001, 2002 e 2003 [2] .

Mesmo considerando o Brasil como um todo, sobressaem-se os quantitativos de 2003, em níveis muito superiores aos de anos passados.

Seguindo a tendência dos incidentes, mostra-se preocupante a escalada de invasões, alavancada pela disseminação e sofisticação dos worms, bem como as fraudes. Estas, no primeiro trimestre de 2004, já atingiram a marca de 796 [3].

1 www.attrition.org , www.alldas.de , www.zone-h.org
2 www.nic.br
3 www.nic.br

2. PROTEÇÃO LEGAL CONTRA CRIMES CIBERNÉTICOS

A sensação corrente de ausência de estatutos legais para promover o combate aos crimes de informática não reflete a realidade, que emerge apenas após analise criteriosa. O mesmo conceito pode ser aplicado quando a intenção é a de estabelecer critérios para elaboração de normas que tratem do assunto da segurança no ciberespaço.

Pode-se dizer que o Brasil possui leis que oferecem a proteção devida contra atitudes indesejadas, mesmo que estas possam ser aprimoradas. A mais recente evolução das leis que tratam do ciberespaço deu-se mediante a aprovação da Lei 9.983 de 2000, que estabeleceu, dentre outras medidas, proteção para sistemas de informações governamentais.

Merece destaque igualmente o asseveramento dos crimes envolvendo crianças e adolescentes, trazido pela edição da Lei 10.764 de 12 de novembro de 2003.

2.1. ETS 185 – Conselho da Europa - Convenção sobre Crimes Cibernéticos

A Convenção sobre Crimes Cibernéticos, apresentada em 23 novembro de 2001 pelo Conselho da Europa, denominada ETS no. 185, devido a sua grande aceitação como modelo internacional de referência para formulação de textos legais, foi empregada neste artigo para comparar e verificar o grau de amadurecimento das leis brasileiras.

Nos itens que seguem, foram extraídas da legislação nacional textos correspondentes às condutas expressas em cada artigo da ETS 185.

ETS 185 Seção 1 – Matéria Penal Substantiva

Título 1 – Crimes contra a Confidencialidade, Integridade e Disponibilidade de Sistemas e Dados em Computadores.

Artigo 2 – Acesso Ilegal

Artigo 4 – Interferência em Dados

Artigo 5 – Interferência em Sistemas

Estas condutas foram consideradas como crimes mediante aprovação da Lei 9.983/2000, apenas para os casos que envolvam dados ou sistemas sob responsabilidade da administração pública, sendo o agente ativo um funcionário público ou outro a este equiparado.

Artigo 3 – Interceptação Ilegal

A Constituição Federal do Brasil de 1988 considera invioláveis as comunicações telefônicas e de dados, exceto para os casos em que haja autorização judicial expressa. Desde 1996, com o implemento da Lei 9.296, interceptações de fluxos de voz ou dados passaram a ser penalizados criminalmente, complementando os ditames constitucionais.

Artigo 6 – Uso Indevido de Dispositivos

Embora visto por grande parcela da população como um ato condenável, a exemplo dos casos de clonagem de aparelhos celulares e disseminação de vírus, esta conduta ainda não pode ser elencada como um crime.

Título 2 – Crimes Vinculados ao Uso de Computadores

Artigo 7 – Falsificações Realizadas com Emprego de Computadores

Artigo 8 – Fraudes Cometidas com Emprego de Computadores

A Doutrina Penal no Brasil se constituiu mediante observação de condutas condenáveis, não importando, em princípio, quais os instrumentos utilizados na prática delituosa.

Assim sendo, o emprego de ardil com a finalidade de obter vantagem econômica indevida, já consta do Código Penal pátrio em artigos como o 171 e 307.

Exemplos recentes e marcantes como as fraudes acometidas contra bancos e seus correntistas, que tem nos e-mails e sítios forjados seus maiores instrumentos, já ocasionaram diversas prisões condenações.

Título 3 – Crimes Vinculados aos Conteúdos
Artigo 9 – Crimes Relacionados à Pornografia com Crianças

A Lei 8.069 de 1990, conhecida como Estatuto da Criança e do Adolescente, introduziu o crime de publicar conteúdo que contenha material pornográfico envolvendo crianças ou adolescentes.

Em sua mais recente atualização, mediante aprovação da Lei 10.764 em 12 de novembro de 2003, estendem-se às condutas aos atos de apresentar, produzir, vender, divulgar e publicar como crimes, desde que envolvam material pornográfico com crianças ou adolescentes.

Título 4 – Infrações aos Direitos de Autor
Artigo 10 – Crimes Relacionados à Violação de Direitos de Autor

Desde 1973, com a aprovação da Lei 5.988, os autores de conteúdos de interesse artístico, literário ou científico tem seus direitos garantidos, estatuto este recentemente atualizado pela Lei 9.610 de 1998.

Em particular, outro estatuto cuida especialmente da propriedade intelectual de software e bases de dados, considerados como conteúdos de interesse peculiar e, portanto, merecedores de código próprio, a conhecida Lei do Software. A sua última atualização decorre da aprovação da Lei 9.609, no ano de 1998.

Título 5 – Culpabilidade e Penalidades Assessórias

Artigo 11 – Tentativa e cumplicidade
Artigo 12 – Culpabilidade da Pessoa Jurídica
Artigo 13 – Penalidades e Demais Medidas

De forma inovadora, o novo Código Civil apresentou o conceito da responsabilidade objetiva. Traduzindo, esta pode ser compreendida como a obrigação da parte contratada em reparar danos causados em função dos serviços que presta, mesmo que não ocasionados de forma intencional, mas considerando que estes deveriam ser previstos quando da oferta dos serviços, não podendo aquela alegar desconhecimento ou despreparo.

A tese pode ser invocada para reparação de dados de usuário que, por exemplo, viu seus dados pessoais, como senhas, dados bancários ou números de cartões de crédito, expostos a pessoas mal intencionadas, sem que o prestador de serviço que os armazenava tivesse empregado medidas básicas de segurança para resguardá-los.

ETS 185 Seção 2 – Matéria Processual

Considerando as previsões básicas da Constituição Federal e do Código de Processo Penal do Brasil, o Poder Público goza de privilégios suficientes para combater os crimes cibernéticos, sendo resguardados ao cidadão sua intimidade e vida privada.

Sobre a antecipação de medidas que visem a preservação de evidências, nada impede que o detentor de dados privativos e voláteis cuide para que sejam mantidos protegidos até a expedição dos devidos mandados de afastamento de sigilo.

Uma premissa básica diretamente relacionada à privacidade estabelece a necessidade de obtenção de ordem judicial quando se fizer necessário investigar dados privativos, ou realizar buscas e apreensões de materiais de informática.

Observa-se que algumas medidas judiciais inovadoras já permitem que policiais acessem diretamente informações de conexões, desde que excluídos quaisquer conteúdos das mesmas. Para o caso da interceptação de fluxos telemáticos em tempo real, exige-se o devido mandado expedido por um magistrado.

ETS 185 Seção 3 – Jurisdição

A Doutrina do Direito pátrio utiliza o *princípio da ubiqüidade* para estabelecer o local de crime.

Este princípio dita que todos os locais onde foram realizados atos constitutivos de um crime sejam considerados locais do crime. Caso quaisquer destes tenham ocorrido em território nacional, será a Justiça Brasileira competente para processar os culpados.

Em tese, portanto, se um simples roteador for empregado como instrumento de crime, estando inserido no espaço territorial brasileiro, poderá a Justiça nacional ser acionada.

ETS 185 Capítulo III – Cooperação Internacional

O tema da Assistência Jurídica Mútua vem ganhando força nos últimos anos, possibilitando a assinatura de diversos acordos.

Desde o ano de 2000, o bloco do MERCOSUL implementou acordos de Assistência Jurídica Mútua entre seus Estados Membros, incorporando avanços significativos na persecução do crime organizado, tráfico de drogas e substâncias ilícitas, bem como do contrabando e descaminho.

Abriu-se igualmente espaço para o combate ao crime cibernético, que demanda extrema fluência entre autoridades transnacionais, superando o tedioso, cansativo porém tradicional processo de solicitação de medidas via Cartas Rogatórias.

Como exemplos destes tratados citam-se adicionalmente aqueles firmados com os Estados Unidos da América e Peru durante o ano de 2001.

Encontram-se em estudo acordos com países de outros continentes, em especial do bloco europeu.

3. INICIATIVAS FEDERAIS VINCULADAS À SEGURANÇA DA INFORMAÇÃO

O Brasil destacou a segurança da informação como tema relevante desde a publicação do Decreto no. 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, criando o Comitê Gestor de Segurança da Informação vinculado ao Gabinete de Segurança Institucional da Presidência da República 4.

O ano de 2003 foi especialmente intenso, sobressaindo-se a criação de diversos grupos de trabalho para cuidar de assuntos como:

- Normas técnicas e regulamentos para a segurança da informação;
- Programa de proteção do conhecimento;
- Criação de Centro de Emergência de Computação da Administração Pública Federal;
- Uso comercial de criptografia;
- Normas para uso e disponibilização da Internet;
- Sistemas operacionais de fonte aberta;

4 www.planalto.gov.br/gsi/cgsi

- Política Nacional de Telecomunicações;
- Pesquisa sobre segurança da informação.

Após a entrega dos relatórios dos Grupos, já em 2004, ficou decidido que, de posse do estudo inicial, o trabalho para criação do Centro de Emergência de Computação deveria prosseguir. Não obstante a condução do tema da segurança cibernética no mundo, este Centro poderá inserir-se na estratégia hemisférica de segurança como um ator governamental na rede de *CSIRT*s das Américas[5].

4. CONCLUSÕES

Os esforços multidisciplinares de órgãos nacionais e internacionais certamente trarão maior proteção aos sistemas de informação e aos usuários dessas redes de informação.

Além de prover medidas jurídicas adequadas, pretende-se criar e apoiar uma cultura de segurança cibernética, atuando junto aos agentes da sociedade civil e dos governos nacionais. Os instrumentos de combate aos ilícitos, como leis, grupos de resposta e tecnologias, só deverão servir apropriadamente se encaixados em um ambiente favorável.

Por se tratar de tema com grande dinamismo, as interações entre agentes deverão ser reforçadas, devendo os resultados passar por exames periódicos possibilitando a evolução das estruturas e conceitos formados.

5. REFERÊNCIAS BIBLIOGRÁFICAS

Blum, Renato M. S. (coordenador) e outros; Direito eletrônico – a Internet e os tribunais, Editora EDIPRO, Bauru – SP – 2001

- Pereira, Ricardo Alcântara; Ligeiras Considerações sobre a Responsabilidade Civil na Internet ;

Delmanto, Celso; Delmanto, Roberto; Delmanto Júnior, Roberto; Código Penal Comentado – Rio de Janeiro/RJ – Ed. Renovar, 1998.

Mandia, Kevin; Prosise, Chris; Incident Response: Investigating Computer Crime – Editoras Osborne/McGraw-Hill – EUA – 2001.

5 www.oas.int

BFW E MAILRELAY – UMA ABORDAGEM PARA FIREWALLS COM BAIXA INTRUSÃO

Leonardo Garcia de Mello

Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – CEP 91.501-970 – Porto Alegre – RS – Brazil
lmello@inf.ufrgs.br

Resumo

Este trabalho apresenta uma proposta para arquitetura de firewalls, a qual foi designada como bfw – de bridge firewalling. Ela foi implementada totalmente em ambiente Linux, e consiste em empregar uma máquina para fazer a filtragem de pacotes em baixo nível (no correspondente ao nível de enlace no modelo OSI, ou no nível físico do modelo TCP/IP), apresentando extrema facilidade para implantação nos mais variados ambientes de rede.

1. INTRODUÇÃO

Para um grande número de organizações, existe a necessidade de manterem-se interligadas por meio de redes de computadores – que por vezes abranjam, até mesmo, grandes extensões territoriais. Isto é algo necessário para a integração de recursos como troca de emails, navegação Web, bem como disponibilização de conteúdos em *homepages* [TAN 97]. Desta forma, elas conseguem dispor de um alto grau de conectividade oferecido por meio de uma ampla infra-estrutura de telecomunicações.

Entretanto, esta mesma conectividade da qual elas podem dispor é um recurso que corre o risco de perceber comprometida em parte, ou mesmo na totalidade, a qualidade dos serviços oferecidos em decorrência de vários tipos de ameaças – tais como ações de *hackers* e viroses de computador [WEB 1989] [WEB 1997]. Sendo assim, faz-se necessária a implantação de soluções que assegurem um elevado nível de segurança durante a utilização dos benefícios oferecidos por redes de computadores.

Para uma organização, entende-se que caso uma tentativa de ataque tivesse sucesso, ela poderia ter um comprometimento bastante sério de seus dados, seus recursos computacionais, ou até mesmo de sua reputação [CHA 95]. Uma das maneiras de proteger-se contra ataques é empregando-se *firewalls*. Entretanto, devido ao porte de grande parte das redes de computadores e a quantidade diária elevada de incidentes; tornam-se difíceis as tarefas de detecção, diagnóstico e execução de contramedida em resposta de forma manual.

Desta maneira iniciou-se o desenvolvimento de uma solução que fizesse isto de maneira totalmente automatizada. Neste artigo, procura-se apresentar a descrição de uma solução implementada totalmente em ambiente Linux utilizando os novos recursos disponíveis no *kernel* da série 2.6 [LIN 2004].

2. FIREWALLS

Conceitualmente, *firewall*s são sistemas compostos por *hardware* e *software* que permitem impor uma política de controle de acesso entre redes. Basicamente, podem ser utilizados para proteger um ambiente de rede do acesso indevido por outras redes.

Fala-se que o *firewall* faz parte de uma *rede interna*, à qual ele protege. Ele serve como portal de acesso entre essa rede interna e uma *rede externa* com a qual é desejado que sejam mantidas restrições. Normalmente, considera-se uma rede interna privada como a protegida, e a Internet como a rede externa. Enfim, *firewall*s podem ser utilizados entre subredes que possuam políticas diferentes.

É função do *firewall* monitorar e controlar o tráfego que ocorre entre as redes interna e externa, servindo como *gateway* para os *hosts* de cada uma. Eles podem oferecer proteção contra ataques a protocolos ou aplicações individuais e têm relativa facilidade de configuração.

Sua maior vantagem consiste em representar um único ponto de controle para a segurança de uma rede interna, sendo o único ponto de administração. Em vez de dispor restrições sobre *hosts* individuais, os administradores podem concentrar seus esforços apenas em uma área [BER 97].

Ainda que não seja um item obrigatório, o *firewall* pode ser utilizado como na Figura 1 [CHA 95]. Sem ele, pode-se dizer que a sub-rede estaria totalmente exposta às ameaças vindas da rede externa. Isso significa que se, por algum equívoco houvesse algum deles mal configurado ou com alguma falha que pudesse ser explorada, estaria suscetível aos ataques externos.

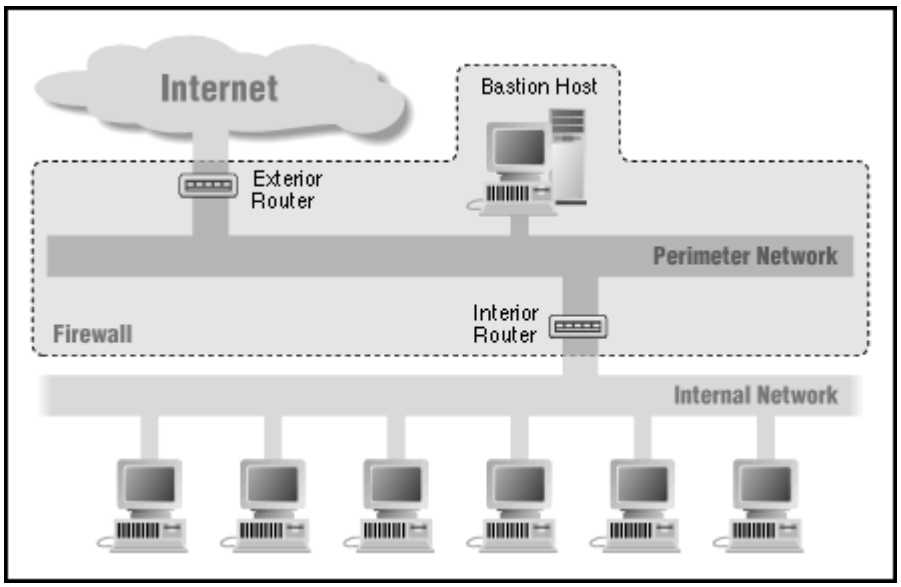


Figura 1 – Disposição de um *firewall*

Na Figura 1, observa-se que além dos elementos *firewall*, rede interna e rede externa; também existe um elemento chamado *Perimeter Network* – por vezes, também referenciado como sendo DMZ (de *DeMilitarized Zone*). A finalidade de uma DMZ é conter todos os *hosts* com serviços acessíveis pela rede externa para que, na eventualidade de um atacante conseguir acesso à um deles, ele fique isolado das máquinas na rede interna. A DMZ não deve conseguir acessar a rede interna.

2.1. Aspectos relacionados ao uso de *firewall*s

Além de controle do acesso, é possível enumerar diversos aspectos que justificam o uso de um *firewall*: proteção contra serviços vulneráveis, acesso controlado à rede interna, segurança controlada, controle estatístico de uso da rede e imposição de uma política de segurança [MEL 2000].

A implantação de um *firewall* pode resolver muitos problemas, mas ainda assim possui uma série de limitações; entre as quais podem ser citadas: o acesso restrito a serviços desejáveis, a possibilidade de contorno do firewall, a falta de proteção contra ataques internos, os ataques dirigidos a dados, e o throughput (vazão) [MEL 2000].

3. DESCRIÇÃO DA SOLUÇÃO BFW

Em termos técnicos a proposta de segurança consiste em instalar, em cada unidade, dois componentes: um do tipo *bridge com firewall* (doravante designada por *bfw*) e outro do tipo *mailrelay*. Estes elementos, *bfw* e *mailrelay*, estão encarregados de realizar as seguintes funções:

- *Firewall* do tipo *bridge* - A implementação de um filtro de pacotes empregando a abordagem de uma *bridge* [TAN 97] permite-nos criar um *firewall* do tipo "caixa-preta", de existência imperceptível e de implantação bastante simples em qualquer ambiente. Isto pode ser feito empregando-se os recursos disponíveis na nova série 2.6 para o *kernel* do sistema operacional Linux. Este recurso apresenta uma inovação da série 2.6, e que não era possível anteriormente a

não ser pela aplicação de *patches* em um *kernel* da série 2.4 [BRI 2004].
Desta forma, é possível implantar a bfw sem a necessidade de qualquer reconfiguração nas máquinas com relação ao endereço IP do *gateway default* [TAN 97]. Também é possível estabelecer planos de contingência para falhas neste equipamento, pois não existe a necessidade de alteração na configuração dos equipamentos da rede local.
Os *softwares* utilizados para filtragem de pacotes são o *iptables* [IPT 2004] e o ebtables [EBT 2004], do Linux, dentro do *framework* tuxfrw [TUX 2004].

- Filtragem de pacotes – a bfw deve dividir o cenário de cada sub-rede em 3 partes, assim designadas: rede externa, rede interna e DMZ (de *demilitarized zone*) [CHA 95]. A rede externa é composta por tudo aquilo o que não pertença à unidade, a DMZ contém apenas algumas poucas máquinas com serviços que devem estar acessíveis pela Internet, e a rede interna é composta por equipamentos sem necessidade de estarem acessíveis pela Internet.

- Detecção de intrusão – utiliza-se uma ferramenta especializada para detecção das tentativas de ataque por *hackers* – o Snort [SNO 2004]. Por meio do Snort, é possível fazer um registro no *syslog* de cada máquina *bfw*, gerar *traps SNMP*, e até mesmo manter um banco de dados com o registro completo das ocorrências.

- Controle do uso da largura de banda – a largura de banda é um recurso computacional que determina o quanto pode existir de tráfego. Pelo modelo *best-effort* empregado atualmente, todo o tráfego é tratado da mesma maneira - sem nenhuma distinção. Em termos técnicos, por meio da bfw é possível alterar a disciplina de filas empregada de FIFO para CBQ [CBQ 2004] ou HTB [HTB 2004]. Nestas disciplinas de filas, existe a definição de classes com base em números IP e endereços de portas.

- *Transparent proxy* para HTTP – a navegação Web, preferencialmente, deve ser feita através de *proxies*. O emprego de servidores *proxy* tem a grande vantagem de permitir o uso de *caching* para conteúdos utilizados com maior freqüência. De maneira que quando algum conteúdo for acessado na Internet por meio do *proxy*, ele também estará disponível por algum tempo para o próximo requisitante desta mesma url [CHA 95].
  Entre as vantagens que podem ser obtidas empregando-se servidores *proxy,* vale a pena citar: serviços proxy são bons para logging, utilizam endereços IP válidos apenas nas máquinas servidoras e os serviços do proxy permitem aos usuários acessarem os serviços da Internet ainda mais "diretamente" (em comparação a outras arquiteturas como *dual-homed hosts*).
  Entretanto, também surgem inúmeras desvantagens relacionadas ao uso de servidores *proxy*: eles podem surgir com atraso para novos serviços, eles requerem diferentes software para cada serviço, e eles tornam necessária modificações nos clientes, nos procedimentos ou em ambos. Além disso, o uso de proxy não é aplicável para alguns serviços, e os serviços proxy não protegem de todas as fraquezas dos protocolos de aplicação [MEL 2000].
  Utilizando a bfw em conjunto com um servidor proxy, é possível direcionar as requisições através de NAT [RFC 1631] para os servidores *proxy* que tenham implementado o suporte à *Transparent Proxies* segundo o padrão da RFC-3040 [RFC 3040][WES 2001]. Para este caso, o servidor *proxy* utilizado foi o Squid.

- *Mail-Relay* Transparente – Este serviço deve operar em conjunto com a *bfw*, funcionando da seguinte maneira: por meio da *bfw*, todo o tráfego de email (porta 25/tcp) é redirecionado por meio de NAT para uma máquina onde há um servidor de *mail relay* com software antivírus. Sem afetar a estrutura atual de servidores, este equipamento está encarregado de inspecionar cada mensagem e seus anexos. A filtragem dos emails com vírus é feita com base em um MTA alternativo – o Amavis [AMA 2004].
  Com isso, é possível encaminhar o tráfego de modo totalmente transparente para um host que faça a verificação da existência de vírus nas mensagens. Ao longo dos últimos anos, o serviço de email tornou-se a principal "porta de entrada" para viroses [WEB 1997].

A disseminação extremamente rápida deste tipo de programa é algo que foi enormemente facilitado pelas versões mais recentes de sistemas operacionais e aplicativos que, ao tentarem oferecer um conjunto de ferramentas para automação de tarefas, tornaram mais fácil para que um vírus realize todo o tipo de ações maliciosas.
Os problemas causados por vírus são conhecidos: destruição de arquivos, lentidão dos equipamentos e envio de mensagens com o remetente forjado. Este projeto propõe o emprego de uma solução a ser aplicada diretamente nos servidores de email – e de forma totalmente transparente, dispensando alterações de configuração.

- Análise de tráfego – com a instalação da solução *bfw*, obtém-se um ponto de controle único. A partir disto, é possível empregar ferramentas para análise do tráfego. Desta maneira, pode-se realizar diagnósticos de problemas de tráfego, identificar gargalos de comunicação e, também, ataques do tipo negação de serviço. Para isto foi utilizado o software ntop [NTO 2004], que fornece praticamente as mesmas informações que poderiam ser obtidas por um agente *Rmon*.

- Atualizações automáticas – Manter um software sempre atualizado é a premissa número um na área de segurança de redes de computadores [WEB 1997]. Isto se deve ao fato de que a maioria das vulnerabilidades dos *softwares* de rede é corrigida através de sua atualização. No entanto, o trabalho de se manter atualizado um enorme conjunto de sistemas instalados é uma tarefa hercúlea se realizada de forma manual e esta é a razão pela qual tantas redes são facilmente invadidas por hackers: seus gerentes não conseguem ter a agilidade requerida e suas redes ficam perigosamente expostas aos ataques. Os sistemas bfw e o mailrelay procuram manter-se sempre atualizados com as versões mais recentes de software através de uma ferramenta especializada - o APT [APT 2004]. O APT foi desenvolvido originalmente para a distribuição Linux Debian, mas atualmente encontra-se disponível para quase todas. Por meio dele, é feita realizar toda a gerência de configuração.

4. MODIFICAÇÕES NO KERNEL

Para que seja possível implementar um *firewall* do tipo *bridge*, é preciso utilizar um *kernel* para o sistema operacional Linux que seja no mínimo da série 2.4. Entretanto, recomenda-se fortemente que seja utilizado um *kernel* da série 2.6 pois a série 2.4 está sendo descontinuada pelos mantenedores [LIN 2004]. Além disso, o suporte à *bridge firewalling* é algo que não existe originalmente para a série 2.4 e apenas está disponível quando ele é recompilado após a aplicação de *patches* apropriados [BRI 2004].

É preciso que o *kernel* da série 2.6 possua habilitado o suporte ao suporte à filtragem de pacotes em nível de bridge. No momento em que o *kernel* for recompilado, é preciso selecionar as opções indicadas na Figura 2 – isto também pode ser feito como módulos.

```
CONFIG_NETFILTER=y
CONFIG_BRIDGE_NETFILTER=y

#
# Bridge: Netfilter Configuration
#
CONFIG_BRIDGE_NF_EBTABLES=y
CONFIG_BRIDGE_EBT_BROUTE=y
CONFIG_BRIDGE_EBT_T_FILTER=y
CONFIG_BRIDGE_EBT_T_NAT=y
...
CONFIG_BRIDGE_EBT_LOG=y
CONFIG_XFRM=y
```

Figura 2 – Opção necessária para bridge firewalling no kernel v2.6

5. FUNCIONAMENTO DA BFW

A *bfw* é um equipamento que possui três interfaces de rede: uma para a rede externa (eth2), uma para a DMZ (eth1), e uma para a rede interna (eth0). Todas essas interfaces são aglutinadas dentro de um novo dispositivo "virtual" chamado de br0, e é ele quem faz o repasse de pacotes entre as interfaces de rede.

Nenhuma das três interfaces de rede precisa ter endereço IP (tal como acontece na abordagem usual, de Chapman [CHA 95]) e não há necessidade de criar-se sub-redes. As interfaces encontram-se em modo promíscuo, e o repasse de pacotes é feito com base nos endereços MAC. A Figura 3 contém uma descrição da interface br0, e os endereços MAC que ela conseguiu assimilar.

Para este caso, existem 3 diferentes domínios de colisão: o primeiro é formado pela interface da rede externa e o endereço do roteador, o segundo é formado pela interface da DMZ e as máquinas neste segmento. O terceiro e último domínio de colisão é formado pela interface da rede interna e os endereços MAC associados.

```
bfw:~ # brctl show
bridge name     bridge id               STP enabled     interfaces
br0             8000.0000214dd5fd       yes             eth0
                                                        eth1
                                                        eth2
bfw:~ # brctl showmacs br0
port no mac addr                is local?       ageing timer
3     00:00:21:4d:d5:fd         yes              0.00
1     00:00:b4:74:13:27         no              86.00
1     00:04:75:8b:59:ef         no              46.55
1     00:04:e2:8e:39:a5         no             250.48
3     00:0b:fd:36:0e:80         no               0.00
2     00:10:4b:36:f0:36         no               0.00
2     00:10:5a:06:c3:70         no               1.26
bfw:~ # ping router -c 1
PING router.prr4.mpf.gov.br (200.142.21.1) 56(84) bytes of data.
64 bytes from router.prr4.mpf.gov.br (200.142.21.1): icmp_seq=1 ttl=255 time=1.18 ms

--- router.prr4.mpf.gov.br ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.184/1.184/1.184/0.000 ms
bfw:~ # arp -a
router.prr4.mpf.gov.br (200.142.21.1) at 00:0B:FD:36:0E:80 [ether] on br0
```

Figura 3 – Estado da interface virtual br0

6. RECURSOS NECESSÁRIOS

O projeto caracteriza-se por reaproveitar equipamentos obsoletos para qualquer outra finalidade, em termos capacidade de processamento. Apenas a título de ilustração, um equipamento utilizado para atender uma rede com cerca de 220 equipamentos é um Pentium MMX com 96 Mb de RAM e a sua utilização consome cerca de 25% da capacidade segundo a métrica *load average*.

Cada bfw necessita ser um PC usando sistema operacional Linux com uma distribuição baseada em RPMS (tal como Conectiva Linux, RedHat Linux ou Suse), 3 placas de rede, disco rígido com pelo menos 2 Gb e o mínimo com 64 Mb de memória. Cada mailrelay deve ser uma máquina com uma placa de rede e disco rígido de no mínimo 2 Gb.

É necessário também, para o mailrelay, um software antivírus. Apesar de existirem soluções gratuitas observou-se que elas não apresentam atualizações na freqüência considerada ideal para grande parte das organizações.

7. CONTRIBUIÇÃO

A abordagem do tipo *bridge com firewall* apresenta a vantagem de poder ser inserida em qualquer ambiente de um modo absolutamente invisível para o roteamento, quando em comparação à abordagem usual de fazer um *firewall* composto por um filtro de pacotes e um servidor *proxy* [CHA 95]. Desta maneira, foi possível criar um *firewall* que pode ser utilizado em qualquer cenário.

Se fosse utilizada uma abordagem convencional de o *firewall* ser o roteador [CHA 95], seria necessário fazer com que todas as máquinas clientes precisassem ter alterada a referência do seu *gateway* padrão [TAN 97]. Apesar de existirem tecnologias que permitam a contingência – tais como HSRP e VRRP – elas ainda apresentam custo bastante elevado.

8. CONCLUSÕES

O projeto *bfw* (*bridge com firewall*) baseia-se em empregar uma máquina usando Linux para funcionar como se fosse um *firewall* do tipo *bridge.* Teoricamente, a *bfw* pode ser instalado em qualquer ambiente e sem a necessidade de alterar as regras para roteamento ou o *gateway* padrão nas máquinas clientes.

Isto torna-se possível porque através dos recursos oferecidos no *kernel* da série 2.6 para o sistema operacional Linux, é possível fazer a filtragem ainda em nível de enlace (para o modelo OSI) ou em nível físico (para o modelo TCP/IP). Com isso, tem-se um *firewall* que pode ser implementado com facilidade em qualquer ambiente de rede.

9. REFERÊNCIAS BIBLIOGRÁFICAS

[AMA 2004] A Mail Virus Scanner. Disponível em: <http://www.amavis.org>. Acesso em mai. 2004.

[APT 2004] APT – Package Management Utility. Disponível em: <http://apt.freshrpms.net>. Acesso em abr. 2004.

[BER 97] BERNSTEIN, T. et alli. **Segurança na Internet**. 1997. Editora Campus.

[BRI 2004] Bridge – Linux Ethernet Bridging. Disponível em: <http://bridge.sourceforge.net>. Acesso em jan. 2004.

[CBQ 2004] Linux Traffic Shapping. Disponível em: <http://freshmeat.net/projects/cbq.init>. Acesso em fev. 2004.

[CHA 95] CHAPMAN, D. B.; ZWICKY, E. D. *Building Internet Firewalls*. Ed. O'Reilly & Associates, 1995, 517p.

[EBT 2004] Ebtables – a filtering tool for bridge firewalling. Disponível em: <http://ebtables.sourceforge.net>. Acesso em jun. 2004.

[IPT 2004] Iptables – firewalling, NAT and packet mangling for Linux 2.4. Disponível em: <http://iptables.org>. Acesso em mar. 2004.

[LIN 2004] The Linux Kernel Archives. Disponível em: <http://www.kernel.org>. Acesso em jun. 2004.

[MEL 2000] MELLO, L. G; WEBER, R. F. Implementação de soluções para segurança de redes. Trabalho de diplomação: Bacharelado em Ciência da Computação - UFRGS, 2000 ,60 p.

[NTO 2004] ntop – Network Traffic Probe. Disponível em: <http://www.ntop.org/ntop.html>. Acesso em jan. 2004.

[RFC 1631] The IP Network Address Translator (NAT). Disponível em: <http://www.ietf.org/rfc/rfc1631.txt?number=1631>. Acesso em ago. 2000.

[RFC 3040] Internet Web Replication and Caching Taxonomy. Disponível em: <http://www.ietf.org/rfc/rfc3040.txt?number=3040>

[SNO 2004] Snort – The Open Source Network Intrusion Detection System. Disponível em: <http://www.snort.org>. Acesso em fev. 2004.

[TAN 97] Tanenbaum, Andrew. *Computer Networks, 3rd edition.* Prentice Hall, 1997, 814p.

[TUX 2004] tuxfrw – Linux Firewall Automation Tool. Disponível em: <http://tuxfrw.sourceforge.net>. Acesso em jun. 2004.

[WEB 1989] Weber, Raul Fernando. Vírus de computador. RITA – Revista de Informática Teórica e Aplicada – Instituto de Informática – UFRGS. Volume I, número 1, outubro de 1989. p. 79-112.

[WEB 1997] Weber, Raul Fernando. Segurança na Internet. RITA – Revista de Informática Teórica e Aplicada – Instituto de Informática – UFRGS. Número 2, dezembro de 1997, p. 7-46.

[WES 2001] WESSELS, D. Web Caching. O'Reilly Press , 2001,318 p.

CONSIDERAÇÕES SOBRE A PRIVACIDADE NO ESPAÇO CIBERNÉTICO

Hélio Santiago Ramos Júnior

Acadêmico de Direito da UFSC

Resumo

O presente artigo desenvolve uma análise geral a respeito da privacidade no espaço virtual, inicia-se uma reflexão histórica a respeito do desenvolvimento social e tecnológico associado à crescente preocupação com a defesa da privacidade no ciberespaço, o texto engloba temas como o direito à privacidade do cidadão e a proteção de dados e informações que se pretende manter preservado ou em sigilo no âmbito da internet, destaca-se também a necessidade de fornecer à população um mínimo de condições para assegurar a liberdade de acesso para que o indivíduo possa se inserir na sociedade da informação e do conhecimento, identifica-se a possibilidade do desenvolvimento de política de privacidade cibernética pelo ordenamento jurídico brasileiro para combater as práticas de atos ilícitos e as violações de privacidade que ocorrem na internet, e, finalmente, apontam-se as alternativas para a proteção da privacidade no ciberespaço concluindo pela necessidade de colaboração internacional no intuito de se obter uma maior eficácia na defesa do direto à privacidade no espaço cibernético.

Palavras-chave: Privacidade no ciberespaço; Direito à privacidade; Acesso à informação; Liberdade de acesso.

1. INTRODUÇÃO

A preocupação com a privacidade na internet pode ser considerada algo recente e tende cada vez mais a se ampliar justamente em decorrência do desenvolvimento de processos acelerados e mais complexos de trocas de informações no ciberespaço.

Esses processos tecnológicos inovadores permitem a observância de que, com o tempo, a sociedade vai se diferenciado e se afasta ainda mais daquilo que ela era no passado. Tal percepção se encontra no determinismo spenceriano segundo o qual se entende que as sociedades evoluem e se transformam com a passagem do homogêneo para o heterogêneo.

A história permite a constatação de que o avanço dos processos de comunicação nas civilizações antigas e anteriores eram muito lento, portanto, incomparável com o momento atual onde se verifica uma constante rapidez na transmissão de informações.

Da mesma forma que a sociedade se dinamiza, o direito precisa acompanhar as tendências modernizadoras no sentido de contextualizar e englobar novas circunstâncias específicas criadas pela tecnologia do mundo digital. É uma verdade que a sociedade se desenvolveu com as inovações tecnológicas e isto modificou não somente os processos e trocas de informações mas também reestruturou e ampliou o comércio entre os diferentes povos. Tanto é assim que o interesse pela internet se torna maior na medida em que sua popularidade aumenta e também na expectativa capitalista de lucro com o ambiente virtual, de modo que se percebe que "*na sociedade global, as informações são agilizadas instantaneamente pela eletrônica. Para isso, utilizam o poder da imagem e a forma de pacotes, comercializando-as em escala mundial*." (RI JÚNIOR, 2002, p.479).

2. A LIBERDADE E O DIREITO À PRIVACIDADE NO AMBIENTE CIBERNÉTICO

A internet corresponde a um dos principais elementos oriundos do processo tecnológico e o seu aparecimento e sua popularidade tornam fácil a obtenção de informações particulares através do espaço virtual.

O ser humano tem direito à privacidade assim como à intimidade de forma que devem ser preservados informações particulares que o indivíduo tenha interesse de manter em sigilo e também não se pode permitir que qualquer conteúdo de uma conversa seja divulgado independente do meio empregado de comunicação e diálogo, pois, em qualquer destas hipóteses, uma violação corresponderia a uma intromissão na vida privada.

A privacidade do indivíduo pode sofrer limitações, tais limites têm a sua origem com o contrato social onde os súditos cedem uma parte de sua liberdade para o soberano com a finalidade de estabelecer uma coexistência pacífica e social mas deve-se levar em consideração que "*o fundamento do Direito é a própria liberdade disciplinadora para o bem individual e para o bem comum e não para o bem dos detentores do poder*". (RÁO, 1999, p.28). Além disso, o Direito e o Estado precisam garantir um mínimo ético na internet, garantindo aos ciber-excluídos condições de participação no acesso à internet para evitar a exclusão digital, pois, evidencia-se que o direito à privacidade no mundo cibernético atinge somente aos que já se encontram integrados a este sistema virtual.

A importância da liberdade se faz presente em sua influência na conceituação de direito de muitos filósofos e pensadores, por exemplo, no pensamento kantiano, o direito seria o conjunto das condições por meio das quais o arbítrio de cada um pode harmonizar-se com o arbítrio dos outros, segundo uma lei universal de liberdade.

O confrontamento da liberdade com os limites impostos para a manutenção da coexistência pacífica e social associado a outros elementos da vida contemporânea causam a liberdade anômica que se trata de "*uma liberdade fora dos parâmetros e sincronizações coletivas usuais*.".(BRÜSEKE, 2001, p.16)

A liberdade e a privacidade do ser humano parecem se reduzir ainda mais em decorrência de diversos fatores que passam a ter maior interesse jurídico, dentre os quais, pode-se mencionar a própria criminalidade violenta. Isto é evidenciado no fato de haver câmeras e espelhos mágicos nos estabelecimentos comerciais, detectores de metais nos bancos, cidadãos morando em condomínios fechados etc.

A violação de privacidade torna-se cada vez mais constante mas a privacidade no espaço cibernético não se resume ao e-mail pois também atinge os *browsers* e programas de bate-papo online.

Em se tratando dos *browsers*, isto é, navegadores de páginas virtuais do tipo WWW, sigla em inglês que significa *World Wide Web*, podem ser gerados problemas de privacidade na medida em que o programa deixa vestígios de quais foram as páginas utilizadas, tais vestígios são comumente denominados de *cookies*.

Em uma breve definição, os *cookies* seriam informações que ficam armazenadas no computador do internauta no momento em que ele visita um site na internet com a finalidade de facilitar o reconhecimento do usuário ou identificar uma situação qualquer preexistente no instante em que retorna a uma mesma página anteriormente visitada para tornar mais ágil e dinâmico o processo de navegação no ciberespaço.

Há mitos a respeito do que são os *cookies*. Segundo ARAYA, os *cookies* não podem capturar informações pessoais de um usuário que não esteja disposto a cedê-las nem podem transmitir vírus, além disso, o servidor não tem acesso mais do que os dados contidos nos *cookies* que ele criou. Porém, cabe mencionar que, conforme ASCENSÃO: "*o tratamento dos dados fornecidos pelo internauta na sua indagação permite insuspeitadas possibilidades de conhecimento por terceiros, que são potenciadas pela elaboração de cookies*." E ele acrescenta que: "*a linguagem Java Script permite dirigir instruções ao disco duro doterminal do internauta, levando-o a executar, no próprio computador do internauta e sem conhecimento deste, operações programadas do exterior*." Ele conclui este assunto dizendo que:"*torna-se evidente a necessidade de assegurar uma reserva que responda amuitas das formas de intromissão possível na vida privada*."(ASCENSÃO, 2002, p. 203).

Dentre as formas de conversa virtual, temos o IRC, *Internet Relay Chat*, dentre os quais destaca-se o programa mIRC, no qual, há a possibilidade de ler as mensagens trocadas do usuário com os demais através da gravação de conversas que ficam salvas em arquivos de extensão LOG.

O *log* das conversas particulares deve ser protegido, porque se trata de uma forma digital de correspondência e se verifica que constitui uma troca de informações pessoais, portanto o acesso indevido ao seu conteúdo certamente representa uma violação de privacidade.

3. E-MAIL, COMÉRCIO ELETRÔNICO E CRIMES CONTRA A PRIVACIDADE NA INTERNET

Torna-se uma prática comum a utilização do meio cibernético para violar a privacidade do internauta, como, por exemplo, através do *spam*, ou seja, do envio de mensagens não solicitadas e, principalmente, destinadas para a prática comercial que envolve a divulgação através de anúncios e propagandas por e-mail.

A propaganda por correio eletrônico constitui um mecanismo de divulgação que apresenta certas vantagens em relação a outras formas de transmitir um anúncio visto que o email passou a constituir um meio de comunicação bastante útil, instantâneo e popular.

Certas empresas que perceberam a dimensão do alcance global, direito, rápido e prático que o e-mail proporciona, passaram a investir no correio eletrônico por visualizar um enorme mercado consumidor, deste modo, começaram a oferecer contas de e-mails gratuitas com uma finalidade lucrativa a longo prazo, e, até mesmo, apostando na lucratividade com a formação de um base de dados de seus usuários através da oferta de um serviço que costuma necessitar do preenchimento de informações pessoais para a sua efetivação pois se verifica que, em muitos casos, a empresa ou site condiciona o fornecimento de produtos ou serviços à prestação de dados pessoais que em geral não são necessários à realização da operação solicitada.

As etapas para se adquirir um e-mail gratuito, normalmente, requer-se a aceitação de um contrato entre a empresa que fornece o e-mail gratuito e o usuário contratante que dispõe sobre a regulamentação do serviço prestado. As empresas devem se preocupar em preservar as informações que são recebidas de seus usuários para não violar a privacidade de seus clientes, se necessário, deverá estar expresso em um contrato que disponha que as informações fornecidas somente poderão ser divulgadas a terceiros desde que haja uma autorização prévia do usuário.

Representa-se um fator de preocupação a possibilidade de se comercializar informações particulares do usuário que é obtida pela empresa que as solicita de modo que deve se ter o cuidado com o armazenamento dos dados como as informações pessoais dos clientes, seus perfis e endereços eletrônicos. Tem-se que a venda de lista de e-mails assim como de informações particulares constituem um real comércio da privacidade e deve ser combatido, mas, "*enquanto o poder público não se sensibiliza para o problema, o comércio passa a ditar o destino da rede, procurando estabelecer a regra da não-regulação pública, permitindo que o próprio setor privado dite as normas que disciplinarão a rede*."(ROVER, 2000, p.88).

Em outro aspecto no âmbito comercial, a privacidade cibernética de empresas representa um grande interesse a ser protegido no mundo jurídico porque elas podem possuir uma base de dados contendo informações a respeito de seus clientes e as violações a estas bases de dados podem provocar grandes colapsos sociais através da insegurança das relações entre as empresas, além de, certamente, prejudicar a sua imagem no mercado, e, conseqüentemente, gerando problemas econômicos e abalando a sua estabilidade no comércio.

Há diversos mecanismos e formas de invadir a privacidade do indivíduo na internet e se obter informações particulares que não se encontravam diretamente à disposição, aqueles que detêm a prática de interceptar dados e obter ilegalmente informações, independente da finalidade ou não de causar um dano ou prejuízo, chama-se tal indivíduo de *hacker*.

Um *hacker* pode descobrir uma senha de e-mail de um determinado usuário e violar a sua privacidade ao ler as mensagens de seu correio eletrônico, deste modo, estará violando a vida privada do indivíduo, mas, na hipótese de violar a privacidade de uma empresa que detêm informações de seus

usuários incluindo senhas e outros dados sigilosos, poderá provocar um prejuízo maior, portanto, deverá haver uma forte tendência em proteger as pessoas jurídicas, muito mais do que em relação à privacidade particular do indivíduo, e em especial àquelas que possuem patrimônio e um certo status no meio social.

Não é necessário ser um *hacker* para violar a intimidade de um indivíduo. Como já foi mencionado, o *spam* é um meio de violação da privacidade. Há programas que enviam uma mesma mensagem instantaneamente para diversos e-mails em pouco tempo. Estes programas auxiliam na prática do *spam*, porém, eles tornam mais prático o trabalho de comunicação das empresas com os seus clientes, mas o seu abuso e uso indiscriminável constitui *spam* e deve ser combatido.

O *spam* vêm se tornando uma prática comum. O indivíduo que mantém correspondências através de seu endereço eletrônico fica sujeito a receber mensagens muitas vezes inúteis contendo informações que não são de seu interesse e, geralmente, estas mensagens são provenientes de seus próprios amigos que enviam mensagens encaminhadas.

As mensagens encaminhadas correspondem à transferência de uma mensagem recebida em seu conteúdo para um outro endereço eletrônico. Torna-se uma prática que vem se repetindo constantemente o encaminhamento de mensagens as quais provocam o *spam*.

Há uma outra prática bem semelhante que favorece *o spam*. Esta se refere às correntes de e-mail, ou seja, também consistem em mensagens encaminhadas mas que têm por finalidade manter um vínculo de continuidade, por exemplo, pode-se tratar da crença em uma simpatia que para a sua realização tem como solicitação a transmissão da mesma mensagem a determinado número de pessoas e ainda consta a premissa de que se não cumprido o requisito a tal bendita simpatia não se concretizaria tendo como resultado o azar. Tais usuários que acreditam e repassam essas mensagens, além de praticarem *spam*, estão incentivando a sua prática na internet.

Por fim, cabe ainda mencionar os *e-mails bomb*. Os *e-mails-bomb* têm por finalidade deixar a caixa de mensagens do indivíduo sobrecarregada, que, além de provocar poluição visual ou virtual e atrapalhar na leitura das demais mensagens, pode impedir a vítima de receber novas mensagens de e-mail na hipótese de o usuário estar com a caixa de mensagens cheia por possuir um serviço gratuito de e-mail que oferece um espaço limitado.

Os *e-mails-bomb* costumam ser mensagens repetidas enviadas contendo arquivos pesados que ocupam grande espaço na caixa de mensagem e, em geral, correspondem a um tipo de *spam* com um fim determinado para a prática do ataque contra a privacidade no espaço virtual, portanto, não é tão comum quanto as outras formas de *spam*.

Em decorrência da prática cada vez mais freqüente do spam, começaram a surgir as chamadas *blacklist*, ou seja, um conjunto de dados que possuiriam em seu conteúdo informações detalhando endereços eletrônicos que seriam responsáveis pela prática comum do *spam*.

Um exemplo de *blacklist* é a ORBL (*Open Relay Black List*), trata-se de uma lista negra que possui um banco de dados que armazena endereços IP de servidores de correio eletrônico mal configurados (*open relays*), que permitem que qualquer um se conecte e envie grandes quantidades de mensagens através deles. Acessando esse banco, os administradores de sistemas podem bloquear mensagens remetidas pelos servidores incluídos na lista negra.

Uma crítica que se pode fazer em relação às listas negras em geral se refere à credibilidade do banco de dados visto que, em geral, estas listas se formam com o resultado de denúncias recebidas que não são verificadas antes de serem divulgadas.

4. A POSSIBILIDADE DE POLÍTICA DE PRIVACIDADE CIBERNÉTICA NO ORDENAMENTO JURÍDICO BRASILEIRO

Há como entender que o direito à privacidade cibernética esteja expresso em dispositivos constitucionais no ordenamento jurídico brasileiro.

Tendo como base o artigo 5º, inciso X da Constituição Federal, tem-se que "sãoinvioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material e moral decorrente de sua violação." A partir deste artigo, pode-se deduzir que a

intimidade passa a ter um sentido amplo, deste modo, ninguém poderá se intrometer na vida alheia, por exemplo, publicando fotos, textos, divulgando segredos pois é vedada a intromissão nas questões particulares de cada indivíduo e esta violação implica em indenização pelos danos que forem causados. Neste sentido, faz-se importante acrescentar uma decisão do STF a respeito do direito à intimidade:

> Decidiu o STF que o direito à intimidade - que representa importante manifestação dos direitos da personalidade - qualifica-se como expressiva prerrogativa de ordem jurídica que consiste em reconhecer, em favor da pessoa, a existência de um espaço indevassável destinado a protegê-la contra indevidas interferências de terceiros na esfera de sua vida privada.[STF, MS 23.669-DF (Medida Liminar) Rel. Ministro Celso de Mello, 12/04/00(DJU 17.04.00)]

Um outro dispositivo que pode servir de suporte à defesa da privacidade cibernética é o inciso XII do artigo 5º da CF/88, segundo o qual: "*É inviolável o sigilo dacorrespondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal*."

De acordo com o que é expresso no inciso XII do art. 5º da CF/88, pode-se interpretar que o sigilo da correspondência abrange também as trocas de informações por correio eletrônico porque se trata de uma forma de comunicação por correspondência mesmo que o meio empregado seja o eletrônico e que o espaço seja o virtual, da mesma forma, que inviolável também deve ser o conteúdo de mensagens trocadas pela internet através de programas de bate-papo como os *browsers* que utilizam *javachat* ou *webirc* além de outros como os programas de IRC, ICQ dentre outros porque todos estes constituem meios de comunicação e, antes de tudo, de correspondência. Uma melhor esclarecimento a respeito deste dispositivo tem-se logo abaixo:

> Trata-se de forma de manifestação pessoal, ou melhor, de pessoa a pessoa. Segundo a doutrina, o significado de correspondência trazido pelo inciso XII, tem sentido amplo. É assim, toda comunicação, escrita e verbal, através do espaço, por carta, telegrama, telefone, radiotelefonia, dados informatizados, radiotelegrafia e outros, abrangendo não só a carta mas os demais instrumentos de comunicação (PIVA, 2000, p.29).

No artigo 151 do Código Penal brasileiro está previsto que a violação de correspondência constitui crime punível com pena de 1 a 6 meses de detenção e multa. Da mesma forma, penaliza quem se apossa indevidamente de correspondência alheia, embora não fechada, e a sonega ou destrói no todo ou em parte. Desta forma, os *hackers* que obtêm senha de e-mails e deletam mensagens de usuários poderiam estar cometendo um crime tipificado no artigo 151 do Código Penal por estarem destruindo uma correspondência eletrônica.

Mesmo que não se tenha sido previsto pelo legislador brasileiro na época a existência de *hackers*, na hipótese de violar direitos e causar danos segundo o artigo 186 do Novo Código Civil que estabelece que: "*aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito*.", nesta situação, eles têm a obrigação de indenizar por praticarem um ato ilícito, desta forma entende-se que "*a obrigação de indenizar é a conseqüência jurídica do ato ilícito (CC, arts. 927 a 954), sendo que a atualização monetária incidirá sobre essa dívida a partir da data do ilícito (Súmula 43 do STF)*" (ASSUNÇÃO, 2002, p.184).

O direito à privacidade sofre limitações no ordenamento jurídico brasileiro, as exceções relativas ao inciso XII do art. 5º da Constituição brasileira são as restrições privativas no caso de estado de defesa e de estado de sítio conforme o art. 136, parágrafo 1º, I, "b" e "c"; art. 139, III, da CF/88.

5. ALTERNATIVAS DE PROTEÇÃO À PRIVACIDADE CIBERNÉTICA

As alternativas para proteger a privacidade no espaço cibernético estão aparecendo e já se nota a adoção de práticas visando a defesa da privacidade dos internautas.

Há atitudes que podem ser tomadas na tentativa de se preservar a privacidade no ambiente cibernético. Uma delas seria através do aperfeiçoamento tecnológico na qual a criação de mecanismos que dificultassem e identificassem o *spam* e que forneçam segurança e proteção nas atividades eletrônicas, neste último caso, pode-se abordar os programas de encriptação do tipo PGP, sigla em inglês que significa Pretty Good Privacy. Sobre o processo de encriptação, cita-se:

> O livre acesso, portanto, o acesso não remunerado de qualquer um às obras (ou quaisquer outros conteúdos, disponíveis em rede evita-se através da criptagem ou codificação das mensagens. É a técnica bem conhecida já das emissões de televisão. O acesso exige um decodificador ou instrumento análogo, que será fornecido a título oneroso.(ASCENSÃO, 2002, p. 84)

Existem formas como o bloqueamento de e-mails para combater o *spam*, mas esta forma somente protege o usuário que passa a receber mensagens constantes de um e-mail específico. Pode-se, em busca de uma forma mais eficaz, bloquear o domínio do e-mail mas isto dificultaria o recebimento de mensagens de outros usuários que possuíssem o mesmo domínio.

Há métodos preventivos de evitar a invasão de privacidade como, por exemplo, a mudança frequente de uma senha de e-mail, a criptografia etc. Para evitar a leitura dos *logs* do mIRC, uma simples medida seria restringir o acesso ao computador através de uma senha de entrada. E, em se tratando de *browsers*, para assegurar a privacidade, é aconselhável deletar freqüentemente os *cookies*.

Há momentos em que a violação da privacidade poderá ser utilizada para uma função nobre ou humanitária, ou seja, trata-se da situação em que uma mensagem não solicitada é enviada com objetivo de praticar uma boa ação, como, por exemplo, ajudar a encontrar pessoas desaparecidas ou objetos roubados, divulgar informações com o fim de salvar vidas fornecendo informações sobre alguma doença nova e grave ou sobre algum vírus de computador ou algo de grande urgência que precisa ser divulgado, combater o terrorismo entre outros.

É possível o entendimento de que a quebra da privacidade com fins nobres e humanitários sobrepõe-se ao direito de privacidade particular, pois em proporcionalidade, a busca pela defesa da vida e a manutenção do bem estar social são bens de valor que em determinadas situações devem prevalecer, por exemplo, quando, em nivelamente com a privacidade do indivíduo, esta última passa a ser de interesse relativamente menor.

Alternativas de proteger a privacidade tendem a ser temporárias e, em geral, não solucionam os problemas referentes à violação de privacidade, necessita-se, portanto, de um justiça criminal virtual internacional para manter a ordem no ciberespaço mas no momento em que se encontra parece impensável a adoção da defesa da tolerâcia zero para os crimes praticados na internet.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ARAYA, Christian Hess. *Derecho a la privacidad y cookies.* Material retirado de meio eletrônico. Disponível em: <http://comunidad.derecho.org>. Acesso em: 21 de junho de 2003.

ASCENSÃO, José de Oliveira. *Direito da Internet e da Sociedade da Informação.* Rio de Janeiro: Forense, 2002. 329 p.

ASSUNÇÃO, Alexandre Guedes Alcoforado et al. *Novo Código Civil Comentado.* 1. ed. São Paulo: Saraiva, 2002. 1843 p.

BRÜSEKE, Franz Josef. *A técnica e os riscos da modernidade.* Florianópolis: UFSC, 2001. 216 p.

LAZZARESCHI NETO, Alfredo Sérgio. *Comércio Eletrônico e Política de Privacidade.* Material retirado de meio eletrônico. Disponível em: <http://www.buscalegis.ccj.ufsc.br>. Acesso em: 21 de junho de 2003.

PAIVA, Mário Antônio Lobato de. *E-mail e invasão de privacidade.* Material retirado de meio eletrônico. Disponível em: <http://www.faroljuridico.com.br>. Acesso em: 21 de junho de 2003.

PIVA, Otávio. *Comentários ao Artigo 5º da Constituição Federal de 1988.* 2. ed. rev. e atual. Porto Alegre: Sagra Luzzatto, 2000. 111 p.

RÁO, Vicente. *O Direito e a Vida dos Direitos.* 5. ed. anotada e atual. por Ovídio Rocha Barros Sandoval. São Paulo: Revista dos Tribunais, 1999. 981 p.

RI JÚNIOR; Arno Dal; OLIVEIRA, Odete Maria de (Orgs). A era da globalização e a emergente cidadania mundial. In: *Cidadania e Nacionalidade: efeitos e perspectivas nacionais - regionais - globais.* Ijuí: Unijuí, 2002. 544 p.

ROVER, Aires Jose (Org.). Direito, Sociedade e Informática: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000. 246 p.

AMBIENTE BASEADO EM AGENTES DE SOFTWARE PARA O AUXÍLIO NA DETECÇÃO E ESTUDO DE ATAQUES EM REDES DE COMPUTADORES

Tamer Américo da Silva, Robson de Oliveira Albuquerque, Rafael Timóteo de Sousa Jr.

Universidade de Brasília, Departamento de Engenharia Elétrica, 70910-900,
Brasília – Brasil
desousa@unb.br, {tamer,robson}@redes.unb.br

Abstract

A avaliação de ataques cibernéticos faz parte do trabalho de especialistas que buscam aprimorar seus conhecimentos buscando formas de defesa contra esses, servindo também como meio de obtenção de evidências capazes de solucionar crimes digitais. Uma das maneiras existentes para isso é a utilização de honeypots. Novas tecnologias permitem que estes sejam acessados mediante o redirecionamento de atacantes que inicialmente investem suas ações contra um servidor real. Entretanto, as soluções atualmente desenvolvidas para esta tarefa possuem limitações não contemplando uma série de necessidades que possibilitam a tecnologia ser amplamente utilizada fora do ambiente acadêmico e científico.

Apresentamos neste trabalho um sistema que auxilia no redirecionamento utilizando agentes de software cooperativos capazes de tomar decisões baseadas em ataques detectados contra um ambiente real. Para avaliar nossa proposta, um ambiente de testes foi criado onde simulou-se vários ataques, demonstrando o redirecionamento destes e a análise dos mesmos utilizando técnicas conhecidas.

1. INTRODUÇÃO

A conexão de uma rede privada à Internet a expõe a uma série de riscos, os quais podem ser minimizados com a utilização de mecanismos de segurança, sendo que para estes oferecerem uma proteção efetiva contra os vários tipos de ataques, é necessário que possuam informações relevantes disponibilizadas de forma que possam ser utilizadas para a detecção destes. Neste contexto, visando facilitar e ampliar o estudo dos vários tipos de ataques foram desenvolvidas ferramentas e arquiteturas associadas à tecnologia de Honeypots [1]. Dentre estas, uma das mais recentes é a denominada Bait and Switch (ou Dynamic re-routing) [2] cujo objetivo é redirecionar ataques investidos contra um servidor de produção para um honeypot. Para isso utilizam sistemas de detecção de intrusão e desempenham funções de gerenciamento do tráfego. Entretanto as implementações pesquisadas para este trabalho, como por exemplo o Bait&Switch [3] e o Hogwash [4] possuem limitações para seu uso em um ambiente real, sendo que um dos fatores observados nestes sistemas é que só é possível a utilização de somente um servidor. Além disso, o servidor e o honeypot devem possuir o mesmo endereçamento MAC e IP, de maneira que o próprio sistema gerencie o tráfego para eles. Outra limitação é que não se pode instalá-los de forma a suportar uma Honeynet [5], dado que é uma arquitetura mais complexa e valiosa que uma estrutura com apenas um honeypot.

Uma solução para tais limitações é a criação de um sistema que seja capaz de efetuar o redirecionamento do tráfego inicialmente destinado para um ambiente de produção para uma Honeynet, levando em consideração a facilidade de sua instalação, configuração, sua adaptabilidade ao meio e a própria escalabilidade do sistema, sendo desejável que o sistema monitore e se configure dinamicamente em relação às mudanças ocorridas no ambiente (inclusão/exclusão de um servidor/honeypot e inicialização/interrupção de um serviço ou do próprio servidor/honeypot) de

maneira que em caso de ataques, o redirecionamento seja sempre efetuado para um honeypot similar ao servidor atacado.

Dado esses requisitos, junto com a relativa complexidade e natureza distribuída necessária para a criação de um sistema deste tipo, o desenvolvimento pode se tornar um problema se utilizadas metodologias convencionais. Como alternativa, visando a produção e o gerenciamento mais eficiente de um sistema com tais características, propõe-se a utilização do modelo baseado em agentes de software, visto que suas características solucionam de forma eficiente o modelo de troca de informações necessárias para que o funcionamento do sistema.

2. MODELO IMPLEMENTADO

A arquitetura do sistema proposto tem como componentes centrais um firewall e um IDS. Para a execução dos testes, utilizou-se dois servidores web e um honeypot. A Figura 1 ilustra a disposição física dos componentes da arquitetura.

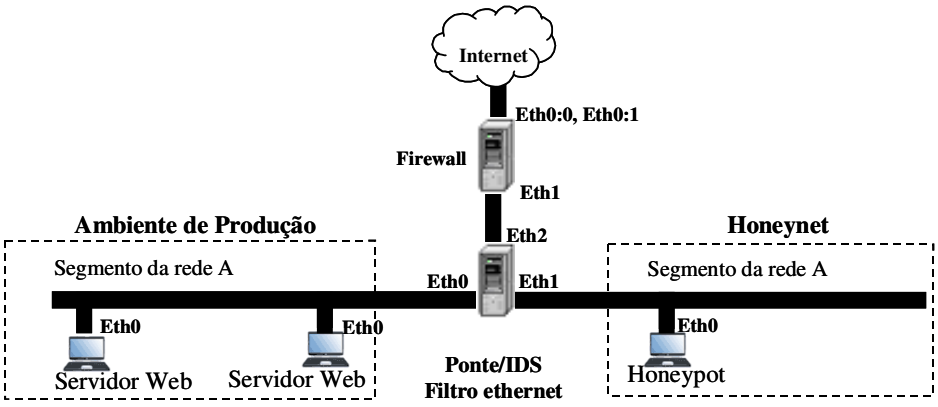


Figura 1 - Arquitetura física do sistema

Ainda utilizando Figura 1 como referência, observa-se que conexão da rede com a Internet é feita através de um Firewall composto por duas interfaces de rede, sendo uma delas definida como eth0 que está ligada à Internet, enquanto que a outra interface, definida como eth1 está ligada na rede interna. O segmento da rede interna, representado na Figura 1 pelo segmento de rede A, contém dois servidores web de produção e um honeypot. Os servidores e os honeypots estão separados fisicamente por uma ponte que contém um filtro de quadros ethernet, que impede o tráfego bilateral entre os dois segmentos da rede A.

O acesso aos servidores de produção através da Internet é feito através de endereços válidos configurados nas interfaces virtuais (eth0:0 e eth0:1) do firewall, cada uma devidamente configurada para redirecionar o tráfego para um servidor web de produção através de regras de mascaramento em execução no firewall.

A arquitetura do modelo foi montada utilizando o sistema operacional Linux e programas de código aberto e livre. Os principais programas envolvidos no sistema são os seguintes: iptables [6] como firewall, snort [7] como IDS, mysql como banco de dados, ebtables como filtro de quadros e o apache como servidor web tanto para os servidores como para os honeypots.

Assim, nesta arquitetura encontram-se instalados agentes de software em todos os dispositivos do sistema (firewall, IDS, servidores e honeypots). A tarefa dos agentes é de tornar possível o redirecionamento dinâmico dos ataques observando os alertas gerados pelo IDS. Através da Figura 2, ilustra-se a tarefa dos agentes decomposta em sub-sistemas cada um sendo executado por uma plataforma de agentes que gerenciam os agentes que nela estão em execução, representadas na figura como componentes do sub-sistema.

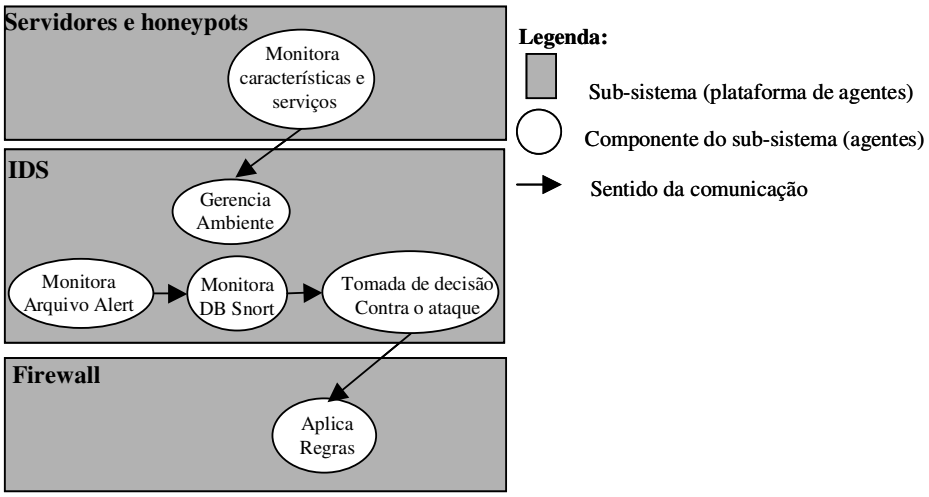


Figura 2 - Comunicação entre agentes e suas ações

A função do agente instalado em um servidor ou honeypot é de coletar informações em intervalos regulares sobre o sistema operacional e os serviços de que estes oferecem e enviá-las para um agente localizado no IDS.

A função do conjunto de agentes no IDS é a de monitorar as tentativas de ataque, gerenciar o ambiente e tomar decisões sobre o tráfego vindo do atacante. O agente responsável pela gerência do ambiente é o responsável por manter atualizada a base de dados sobre os servidores web e honeypots. Para isto, ele recebe informações dos agentes localizados nestas máquinas e efetua a inclusão desses dados em um banco de dados. O monitoramento do tráfego malicioso é feito por um outro agente que verifica o arquivo de alertas do sistema de detecção. Quando algum evento é registrado neste arquivo este agente informa o agente responsável pela tomada de decisões. Uma vez recebida uma mensagem informando alteração no arquivo de eventos, inicia-se a coleta de informações sobre o(s) ataque(s) pesquisando na base de dados por eventos registrados pelo IDS. Efetua-se então uma pesquisa procurando por ataques recentes, baseando-se no tempo de chegada da mensagem que informou a mudança no arquivo de eventos. Desta pesquisa obtém-se os endereços IP de origem do ataque e destino, que são encaminhados para um outro agente, cuja função é a de solicitar o redirecionamento ou rejeição deste endereço IP de origem ao agente localizado no firewall. Para tomar essa decisão, o agente deve inicialmente obter informações sobre a máquina que está sendo atacada. Para isto ele consulta a base de dados de informações sobre servidores através do endereço IP do servidor web. De posse dessas informações efetua-se uma nova pesquisa à procura de um honeypot com as mesmas características. No caso de se encontrar uma máquina compatível, solicita-se ao agente localizado no firewall pelo redirecionamento do tráfego ou caso contrário solicita-se a rejeição do tráfego do atacante a qualquer máquina do ambiente.

Para a concepção do código do sistema utilizou-se como principais ferramentas de desenvolvimento a linguagem Java [8] e a plataforma de agentes Jade [9]. A comunicação entre os agentes desenvolvidos seguiu o padrão de comunicação criado pelo grupo de pesquisa FIPA [10].

3. RESULTADOS DA SIMULAÇÃO

Para a obtenção dos resultados, simulou-se uma seqüência de ataques provenientes de um computador localizado fora da arquitetura protegida para um servidor web da arquitetura, observando o comportamento do sistema durante o período de detecção, redirecionamento e análise dos ataques registrados no servidor e honeypot.

Uma vez executado e detectado o primeiro ataque, o IDS registrou a ocorrência em seu arquivo de eventos. Uma vez esta alteração detectada pelo agente do sistema, desencadeou-se uma série de ações envolvendo os outros agentes, como descritos anteriormente no ítem 2, criando por fim dinamicamente uma regra no firewall que redirecionará o tráfego do atacante para um honeypot. A

Figura 3 ilustra o atacante, os dispositivos de segurança da arquitetura e os servidores envolvidos no ataque.

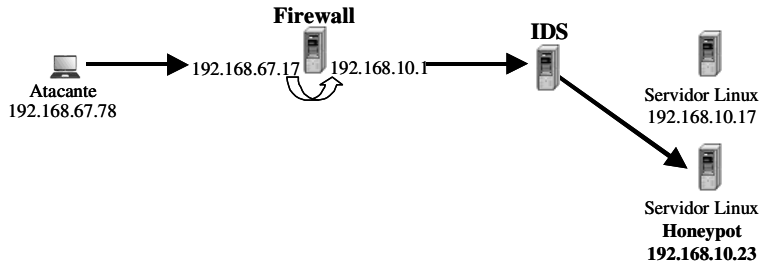


Figura 3 - Redirecionamento do atacante

Com as informações obtidas sobre o servidor e o honeypot, o agente no IDS enviou a seguinte mensagem ACL ao agente no firewall:

```
(INFORM
 :sender  ( agent-identifier  :name avaliaEventos@ids:1099/JADE
                              :addresses (sequence http://ids:7778/acc ))
 :receiver  (set ( agent-identifier  :name aplicaRegras@firewall:1099/JADE
                              :addresses (sequence http://192.168.10.1:7778/acc )) )
 :content "redirect (ipsrc: 192.168.67.78,ipdst:192.168.10.17,iptodst:192.168.10.23)"
 :language  PlainText
:ontology  Pandera )
```

Uma vez recebida a mensagem, o agente processou o conteúdo da mensagem executando em seguida a regra para o redirecionamento do tráfego:

```
Chain PREROUTING (policy ACCEPT)
target          prot opt     source              destination
DNAT       all  --  192.168.67.78       192.168.10.17      to:192.168.10.23
```

Após a detecção do primeiro ataque efetuou-se novos ataques com o objetivo de demonstrar que todos os ataques seguintes serão executados contra o honeypot, disponibilizando-se assim os meios de se coletar informações sobre esses. Assim, neste teste executou-se mais quatro ataques, até o momento em que conseguiu-se obter sucesso na última tentativa, esta efetuada através de um programa específico para gerar uma negação de serviço ao servidor tornando-o indisponível.

Como desejado, nenhum dos ataques efetuados pelo atacante chegou ao servidor web inicialmente atacado. Para essa verificação, analisou-se o arquivo de log de requisições HTTP. O arquivo de log do servidor web contém somente as informações referentes ao primeiro ataque, o qual foi detectado pelo IDS:

```
192.168.10.17 - - [05/Jul/2004:00:30:27 –0300] "GET /bad.cgi?doh=../../../../bin/ps%20-aux HTTP/1.1" 404 1044 "-" "-"
```

Já o servidor honeypot designado para o atacante registrou novas solicitações HTTP provenientes do redirecionamento, como comprovadas analisando-se o log de requisições HTTP. Abaixo temos o conteúdo do arquivo de log onde observa-se os ataques posteriores a detecção do primeiro ataque:

```
192.168.10.23 - - [05/Jul/2004:00:30:35 –0300] "GET teste.php=<!%20--#include%20virtual="http://host2/fake-article.html"-->" 400 977 "-" "-"
192.168. 10.23 - - [05/Jul/2004:00:30:36 -0300] "GET cgi-bin/bad.cgi?doh=gcc%20Phantasmp.c;./a.out%20-p%2031337;" 400 977 "-" "-"
192.168. 10.23 - - [05/Jul/2004:00:30:39 -0300] "http://host/cgi-bin/bad.cgi?doh=Xeyes%20-display%20192.168.22.1;" 501 985 "-" "-"
```

Com exceção do último ataque, que não pode ser registrado no arquivo de log, pois impossibilitou o servidor de gerar seus registros, bloqueando o servidor tornando-o indisponível de responder as requisições HTTP e incapacitando-o de efetuar outras tarefas do sistema operacional, como por exemplo a gravação do arquivo de log. O honeypot teve que ser reiniciado para voltar ao seu funcionamento normal.

O tempo necessário para a tomada de decisão para o primeiro ataque executado foi calculado observando o período compreendido entre a detecção do ataque feito pelo IDS e a execução da regra de acesso no firewall. Observado o registro deste, o que levou no máximo três segundos (de acordo

com a configuração estabelecida), o restante do processo levou aproximadamente 2 segundos, desta forma totalizando um tempo máximo de 5 segundos para tratar o atacante.

4. CONCLUSÃO

Após a montagem e configuração da arquitetura, e a implementação do sistema de agentes de software para interagir com esta arquitetura, foi possível demonstrar que a proposta de se redirecionar um tráfego considerado malicioso de uma rede de produção para uma honeynet pode ser eficiente, sendo interessante do ponto de vista que se retira qualquer possibilidade de novas investidas por parte do endereço de origem de um atacante ao ambiente crítico submetendo seu tráfego para um ambiente de pesquisa com as mesmas características do sistema operacional atacado, o qual poderá dar continuidade a seus ataques com pequenas chances de perceber seu redirecionamento, sendo então alvo de análise posterior de especialistas em segurança. Com a execução dos testes realizados neste trabalho, observou-se que o ambiente proposto contemplou as exigências da proposta.

Além disso, a infra-estrutura projetada e implementada neste trabalho demonstrou que, através da combinação de algumas tecnologias de segurança (firewall, sistemas de detecção de intrusão e honeypots) auxiliadas por agentes de software, é possível obter um ambiente mais integrado e escalável. Nesse contexto, entende-se como integrado por ser o ambiente composto de vários dispositivos funcionando com o propósito de prover segurança ativa e dinâmica, pois existe um trabalho colaborativo entre as partes; e escalável por não ser limitado aos recursos atuais podendo ser acrescentados outros dispositivos, como por exemplo, novos servidores de produção, honeypots, sistemas de detecção de intrusão, sistemas de sobrevivência de rede e balanceamento de carga [11], sendo todos possuidores de agentes de software em suas configurações.

A engenharia de software baseada em agentes se mostrou uma alternativa viável neste trabalho demonstrando maturidade e competência no desenvolvimento de sistemas críticos de segurança de redes. Embora seu uso seja restrito a determinadas aplicações bem definidas, o nível de pesquisa em que se encontram vários trabalhos consultados demonstra que esta barreira deverá ser quebrada em breve. Isto de certa forma comprova que se trata de uma tecnologia promissora e em crescimento que em breve estará ganhando mais espaço no mercado. Além disso, o desenvolvimento dos agentes utilizando o *framework* JADE também se mostrou um fator diferencial, tendo este demonstrado que sua implementação é robusta e pode ser utilizada sem grandes problemas para a geração de agentes baseados no modelo FIPA. Embora alguns problemas ainda devam ser resolvidos, não são fatores que limitem o uso da ferramenta, tendo um objetivo bem definido.

É importante ressaltar ainda que todas as ferramentas utilizadas para o desenvolvimento do ambiente e sua configuração são de uso livre e gratuitos na Internet. Isto gera uma perspectiva de boa qualidade de serviço com o uso de recursos financeiros limitados.

Dentro do contexto deste trabalho, ainda foram avaliadas algumas ferramentas que integram dispositivos de segurança como o firewall e o IDS com o objetivo de alterar as rejeitar novas conexões de um atacante. O principal diferencial da solução apresentada neste trabalho é que nenhuma outra ferramenta utiliza uma estrutura de redirecionamento dinâmico de tráfego malicioso para honeypots baseados nas características do servidor atacado e utilizando agentes de software.

A ferramenta desenvolvida ainda pode evoluir com a integração de várias outras funcionalidades. Existem vários pontos em aberto que necessitam de um estudo mais aprofundado e uma melhor otimização, caracterizando os trabalhos futuros a serem implementados nos seguintes temas:

- Ferramenta de gestão do ambiente. Os agentes necessitam de uma gestão centralizada, de onde o administrador possa ver a situação das informações sendo trocadas pelos agentes e reconfigurar os mesmos se necessário;
- Ferramenta de detecção de intrusão nos servidores de produção. Agentes auxiliariam na detecção de ataques nos próprios servidores, quando estes não forem detectados pelo IDS da rede, podendo assim eles mesmos informarem os agentes no Firewall e no IDS para que estes redirecionem o tráfego ou o bloqueiem.

- Dinamismo na caracterização dos honeypots [12] auxiliados por agentes, de forma que sejam capazes de se executarem serviços de acordo com as características dos servidores de produção.
- Melhoria na performance e segurança na troca de informações [13]. A troca de informações dos agentes é a principal forma de comunicação. Sua troca deve ser confiável, efetiva e bem realizada para que os agentes não tomem decisões erradas mediante o atraso ou a não entrega de informações.
- Integração com o sistema de balanceamento de carga dinâmico [11] também desenvolvido baseado em agentes de software usando a plataforma JADE.

Desta forma, este trabalho, associado com os trabalhos futuros, pode se tornar uma ferramenta de uso efetivo em organizações e instituições de ensino e/ou pesquisa onde exista a necessidade de redirecionamento de tráfego e sua posterior análise.

Além disto, o uso efetivo de agentes inteligentes pode ser considerado com válido e de possível implementação para o auxílio de manutenção e administração de sistemas de informação.

5. REFERÊNCIAS BIBLIOGRÁFICAS

[1] Lance Spitzner , "Honeypots: Tracking Hackers", Addison-Wesley Pub Co, 2002
[2] Joseph Corey , http://www.phrack.org/fakes/p62/p62-0x07.txt
[3] Jack Whitsitt, Alberto Gonzalez , Bait&Switch, http://violating.us/projects/baitnswitch
[4] Jason Larsen, Alberto Gonzalez, Hogwash, http://hogwash.sourceforge.net/
[5] The Honeynet Project , "Know Your Enemy : Learning about Security Threats ", Pearson Education, 2ª edição, 2004
[6] NetFilter/Iptables, http://www.netfilter.org/
[7] Marty Roesch , Snort IDS, http://www.snort.org
[8] James Gosling, JavaTM Technology, http://java.sun.com
[9] F. Bellifemine, G. Caire, A. Poggi, G. Rimassa, "JADE - A White Paper", http://jade.tilab.com/
[10] FIPA- Foundation for Intelligent Physical Agents, http://www.fipa.org
[11] - Robson de Oliveira Albuquerque, Rafael T. de Sousa Jr., Tamer Américo da Silva, Ricardo S. Puttini, Cláudia Jacy Barenco Abbas, "Load Balancing and Survivability for a Network Service using intelligent agents software ", A. Laganà et al. (Eds.): ICCSA 2004, LNCS 3043, pp. 868-881, 2004
[12] Lance Spitzner , Dynamic Honeypots, http://www.securityfocus.com/infocus/1731, 2003
[13] N. Lhuillier, M. Tomaiuolo, G. Vitaglione, "Security In Multi-Agent Systems: Jade-S Goes Distributed", http://exp.telecomitalialab.com/upload/issues/v3n3.pdf, 2003

ATAQUES ELETRÔNICOS DIRECIONADOS A CLIENTES DE INSTITUIÇÕES FINANCEIRAS – PHISHING SCAM

Evandro Mário Lorens

CAIXA ECONÔMICA FEDERAL

Resumo

Introduz conceitos relacionados a ataques eletrônicos, com enfoque nos ataques direcionados a usuários finais. Apresenta especificidades dos ataques phishing scam tais como conceito, modo de operação, estatísticas, tipos e medidas de prevenção. Conclui mostrando tendências e reforçando o papel da educação dos usuários no processo de segurança da informação

1. ATAQUES ELETRÔNICOS

Ataques eletrônicos podem ser classificados como ameaças[1] relacionadas ao mau uso da tecnologia. A exploração de vulnerabilidades[2] tecnológicas através de ataques eletrônicos pode causar danos, prejuízos e violações à segurança da informação.

Para bem entender os ataques eletrônicos, via de regra, deve-se entender o comportamento e as motivações dos atacantes. Esses dois fatores expõem o ponto de partida para o fenômeno dos ilícitos digitais, que evoluem lada a lado ao desenvolvimento tecnológico, especialmente a conectividade e a Internet.

A ausência de um contexto social com regras bem definidas nas relações virtuais sugere que indivíduos agem de modo mais desinibido, diferentemente da maneira como se posicionam nas relações físicas, sem incorrer em preocupações com imagem social, adotando, por vezes, comportamentos não cordiais ou pouco éticos. Outros aspectos psicológicos também contribuem para o perfil de pessoas que se envolvem em ataques eletrônicos: a falta da individualidade, a adoção de personalidade de grupo, a inspiração em exemplos e a ausência de valores éticos consolidados ou ajustados.

Dentre as principais motivações para o engajamento em ataques e crimes eletrônicos destacam-se os ganhos financeiros, desafios pessoais, auto-afirmação perante grupos sociais, vingança, insatisfação profissional e curiosidade.

Os atacantes aos ambientes tecnológicos das organizações são, principalmente, pessoas internas às próprias organizações ou que com elas têm alguma relação. São empregados, prestadores de serviço, fornecedores, vendedores, usuários, clientes e familiares de empregados [BOSWORTH, 2002]. Ataques de origem interna às organizações usualmente se beneficiam das condições de acessos válidos ou facilitados aos ambientes computacionais e por isso, nem sempre são sofisticados em elaboração.

[1] O conceito de ameaça pode ser identificado como uma circunstância ou evento passível de causar dano ou violação de segurança [SUMMERS, 1997].

[2] Uma vulnerabilidade tecnológica é uma fraqueza de um sistema computacional que permite que a segurança da informação seja violada.A origem de uma vulnerabilidade pode residir no projeto do sistema computacional, na implementação ou nos procedimentos de gerenciamento do sistema [SUMMERS, 1997].

Mais complexos, os ataques de origem externa às organizações percorrem basicamente três estágios: preparação ou planejamento, ataque propriamente dito e cumprimento da missão [SUMMERS, 1997].

A fase de preparação consiste basicamente em definir e conhecer o alvo, levantando todos os seus pontos de contato e vulnerabilidades exploráveis. Nesta fase, um minucioso trabalho de pesquisa para coleta de informações institucionais e técnicas pode indicar as possibilidades de penetrar e subjugar o ambiente da organização alvo. Pode envolver ainda muita leitura, capacidade dedutiva e indutiva do pesquisador, além de habilidades psicológicas, tais como a aplicação de engenharia social[3]. É nessa fase que se escolhem ou se desenvolvem as ferramentas que se aproveitarão das vulnerabilidades descobertas, incluindo aquelas que permitirão a remoção de rastros digitais. Efetivamente, define-se a estratégia de todo o ataque.

No estágio do ataque propriamente dito é que os planos de invasão são executados, geralmente visando à tomada de controle do ambiente tecnológico alvo e a geração de permissões tecnicamente legítimas, com altas prerrogativas, de modo a propiciar futuros acessos "pela porta da frente".

A etapa de cumprimento da missão reflete a consecução efetiva do intento planejado, o que pode ser o bloqueio dos serviços, a destruição ou roubo de informações, a instalação de códigos maliciosos, bombas lógicas ou coletores de informações, destruição de evidências de ataques, comprometimento de mecanismos de criptografia, fraudes financeiras, dentre outros.

As motivações dos ataques eletrônicos externos estão, via de regra, relacionadas com a obtenção de vantagens. Reconhecimento e fama, quebra de desafios e ascensão social em grupos, nos últimos anos, têm perdido terreno frente aos interesses em obtenção de ganhos financeiros, que têm crescido substancialmente, especialmente estimulados pelas aparentes facilidades de conquistas, o anonimato e a impunidade do contexto virtual.

Outro fator importante que tem despertado o interesse por ataques eletrônicos voltados a ganhos financeiros é o crescimento significativo da quantidade e diversidade de serviços eletrônicos envolvendo transações financeiras. Cada vez mais, as organizações se tornam dependentes da tecnologia e da Internet para relações com bancos, governo, fornecedores e clientes, vendas diretas, acessos remotos, trabalho colaborativo, dentre outros.

Analogamente às práticas espúrias do mundo físico, um ataque eletrônico visará sempre o ponto mais fraco da cadeia de participantes de uma relação virtual de interesse, ou o "elo mais fraco da corrente", como alvo focal. Essa é uma forma adaptada da lei do menor esforço, objetivando agilidade, comodidade e maior chance de sucesso no intento de um ataque eletrônico.

Considerando como exemplo de cadeia de relacionamento virtual o canal Internet disponível aos clientes de uma instituição financeira, é alta a probabilidade de que a infra-estrutura do lado do banco conte com padronizações e configurações seguras, ferramentas de proteção e monitoramento, mecanismos de autenticação rigorosos e profissionais empenhados em mitigar tentativas de ataques incidentes. Do outro lado do canal, existem clientes diversos, com culturas de segurança diversas, apoiados sobre infra-estruturas básicas, tão somente voltadas à funcionalidade e à facilidade de uso. São os elos fracos da corrente. A maior atenção, estruturação e proteção das organizações aos seus ambientes tecnológicos, a maior divulgação de problemas e soluções de segurança e, a integração de especialistas em segurança da informação aos quadros profissionais das organizações, têm feito com que os atacantes migrem a incidência de suas investidas para os usuários finais e seus computadores.

Valem contra os usuários comuns as mesmas metodologias tradicionais de abordagem para os ataques eletrônicos, guardadas particularidades relevantes, tais como:

- os impactos de um ataque eletrônico são atômicos – atingem habitualmente pessoas ou pequenos grupos de pessoas;

- a detecção de ataques pelo usuário ou técnicos de manutenção é difícil de se realizar, especialmente se o atacante age discretamente na preparação e no ataque propriamente dito, porque o conhecimento de segurança da informação desses agentes é baixo;

- o rastreamento é improvável porque o conhecimento de segurança da informação dos usuários e técnicos de manutenção é baixo e, ferramentas adequadas são escassas, mal configuradas ou simplesmente não existem;

- a preservação de evidências quase nunca ocorre – normalmente ao descobrir "problemas" no computador, a opção imediata do usuário e de técnicos em manutenção é reinstalar o sistema;

- as vulnerabilidades dos sistemas operacionais e aplicativos são abundantes porque usualmente a concepção de sistemas comerciais orientados a usuários prioriza as funcionalidades e a interface, relegando a segurança do software ao plano secundário;

- a instalação de correções de segurança e atualizações dos sistemas pelos usuários não faz parte das rotinas de uso do computador;

- as configurações de segurança dos sistemas, por padrão, vêm habilitadas em baixo nível, com o objetivo de facilitar a instalação e o uso, permanecendo habitualmente dessa maneira;

- usuários finais são altamente suscetíveis aos ataques de engenharia social, especialmente aqueles construídos a partir da oferta de algum tipo de vantagem através da Internet; e,

- não existe uma preocupação maior por parte dos usuários com a origem ou veracidade das informações que lhe chegam ou que consta dos sítios pelos quais navega.

A partir do segundo semestre de 2003, a opção de atacantes veteranos e novatos em todo o mundo tem convergido significativamente para os usuários finais, através da modalidade *phishing scam*, que requer pouco investimento financeiro, implica baixo risco, conta com as particularidades dos usuários já relacionadas e se utiliza de Engenharia Social, como veremos a seguir.

2. PHISHING SCAM

2.1. O que é Phishing Scam?

O termo *scam* refere-se a mensagens de correio eletrônico não solicitadas, de natureza fraudulenta ou enganosa [INFOSEC, 2004]. *Phishing* é uma categoria específica de *scam* em que o atacante envia mensagens de correio eletrônico falsas utilizando imagens institucionais de organizações e textos enganosos com o objetivo de capturar (ou "pescar") informações pessoais e financeiras dos destinatários [SEARCHSECURITY, 2004].

As classes de organizações normalmente usadas pelos atacantes como "isca" para o *phishing scam* são aquelas reconhecidas publicamente, tais como órgãos governamentais, instituições financeiras, administradoras de cartões de crédito, companhias aéreas, empresas de comunicação (rádio, TV, jornais, revistas), concessionárias de serviços públicos, empresas de tecnologia, provedores de acesso à Internet e ainda, sítios de comércio eletrônico, cartões de saudação e encontros virtuais. A lista cresce à medida que novos e diferentes serviços em rede vão se tornando comuns aos usuários.

2.2. Modo de operação

As mensagens falsas de *phishing scam* são construídas com o objetivo de induzir os usuários destinatários a fornecer informações pessoais e financeiras. As razões apresentadas são variadas, podendo explorar questões de segurança, atualização de *software*, confirmação cadastral, habilitação a

prêmios e sorteios, *download* gratuito de sistemas, exigências legais, promoções comerciais. Além das justificativas que pretendem convencer os usuários receptores das mensagens, tenta-se embutir urgência à solicitação e conseqüências desfavoráveis, caso a solicitação de informar os dados pessoais não seja atendida. Prega-se bloqueio de contas e acessos, perda de prêmios, constituição de ilegalidade e mesmo "exposição a vírus e ataques eletrônicos" para aqueles que não atenderem à urgente convocação. Por fim, no corpo das mensagens, apresentam-se *hiperlinks*, sobre os quais o usuário destinatário deverá clicar para fornecer suas informações. Em geral, os *hiperlinks* apresentados são disfarçados para soarem genuínos aos destinatários.

Para proporcionar maior credibilidade à origem das mensagens, o emissor de um *phishing scam* produz falsificação também do endereço de origem, podendo esta elaboração ser mais ou menos sofisticada, dependendo da habilidade técnica do atacante com os protocolos de correio eletrônico e cabeçalhos identificadores das mensagens.

Assim que o usuário receptor procede ao clique solicitado, variadas operações podem ocorrer. A seleção feita pode, dentre outros efeitos perniciosos:

- iniciar a instalação de um programa malicioso no computador, seguida da apresentação de uma mensagem de erro (por exemplo, "serviço temporariamente indisponível") ou redirecionamento ao sítio verdadeiro;

- abrir páginas falsas com formulários para coleta de informações;

- substituir o arquivo *hosts* do computador do usuário, incluindo associações de endereços fraudulentos às URL de sítios bancários ou financeiros;

As informações roubadas através de *phishing scam* são usadas em transferências bancárias de fundos, uso dos dados de cartões de crédito para comércio eletrônico não autorizado, clonagem de cartões financeiros, uso indevido de contas de acesso a serviços eletrônicos, acesso ilegítimo a aplicações corporativas, acesso não autorizado a contas de correio eletrônico, espionagem industrial, uso indevido de dados de identidade, dentre várias possibilidades adicionais.

2.3. Estatísticas

Ainda não existem muitas estatísticas sobre os ataques de *phishing scam* porque constituem uma modalidade de ataque eletrônico que apenas recentemente ganhou notoriedade. Os números existentes deixam a desejar, especialmente porque se estima que mesmo para os ataques tradicionais, os números reais são pelo menos oito vezes mais freqüentes que os números reportados [SLEWE, 2004].

O sítio Web FraudWatch International (www.fraudwatchinternational.com), baseado em Melbourne, Austrália, e voltado à educação, prevenção e investigações em fraudes pela Internet iniciou março de 2004 o levantamento de casos de *phishing scam*. Os casos reportados em abril de 2004 superaram os do mês anterior em 250% e os do mês de maio superaram os casos de abril em 215% [FRAUDWATCH, 2004].

O Anti-Phishing Working Group (APWG), uma associação baseada em São Francisco, EUA, formada por organizações do segmento financeiro e de telecomunicações, apontou crescimento de ataques únicos de *phishing scam* reportados em todos os meses 2004, conforme a tabela abaixo:

MÊS	PHISHING ÚNICOS REPORTADOS	CRESCIMENTO
JAN / 2004	175	--
FEV / 2004	282	61%
MAR / 2004	402	43%
ABR / 2004	1125	180%
MAI / 2004	1197	6%

Fonte: Anti-Phishing Working Group Phishing Atack Trends Report May 2004. [APWG, 2004]

No Brasil, o principal levantamento de ataques eletrônicos é feito pelo NIC BR Security Office. Segundo o NBSO, em 2003, os ataques relacionados a fraudes reportados representaram em média 1% do total dos ataques, num universo em que são considerados ataques *worms* (média anual de 61%), *scan* de portas (34%), ataques a usuário final (1%), dos (0%), ataques a servidor web (0%) e invasão (0%). Nos seis primeiros meses de 2004, os ataques relacionados a fraudes passaram a representar em média 3% de todos os ataques reportados. Destes ataques relacionados a fraudes, mais de 90% foram reportados como *phishing scam* [NBSO, 2004].

2.4. Tipos de phishing scam

Phishing scam tradicional

As mensagens enganosas são construídas com o propósito de convencer o usuário a abri-la e clicar no *hiperlink* disposto no corpo da mensagem. Seguem princípios como o uso de títulos atraentes ou chamativos, falsificação do endereço do emissor, uso de textos e imagens nos padrões das organizações usadas como isca, disfarce do *hiperlink* espúrio para exibi-lo insuspeito [FRAUDWATCH, 2004].

O uso de imagens das organizações nos conteúdos das mensagens é uma tarefa relativamente simples. Ao navegar pelo sítio da organização, pode-se copiar livremente para o equipamento local as imagens, estilos e fontes de texto, hiperlinks genuínos. Copiados os objetos, montá-los convenientemente em uma mensagem de correio em HTML é relativamente trivial.

Eventualmente, algumas mensagens trazem, além das imagens e conteúdos enganosos, *hiperlinks* apontando para páginas no sítio verdadeiro da organização isca. "Fale conosco", "Página Inicial" , "Home", "Política de Privacidade" são alguns exemplos dessas referências. É uma maneira de ganhar a confiança do usuário receptor, aparentando originalidade e estabelecendo falso vínculo.

Alguns produtos antispam que operam por filtros baseados em palavras-chave podem ser ludibriados pela substituição de caracteres nas palavras chave, tais como "O" por "0", "I" por "1", ou, simplesmente, por erro proposital na grafia de palavras chave.

Por estranho que pareça, algumas mensagens falsas incorporam erros gramaticais e de ortografia em seus textos, usam imagens distorcidas ou visivelmente forjadas. Em outras, não há preocupação em disfarçar o *hiperlink* preparado ou o endereço do verdadeiro emissor.

As páginas Web falsas para onde são direcionados os *hiperlinks* das mensagens falsas são construídas de maneira a parecerem originais aos usuários receptores. O principal obstáculo para o atacante é o endereço ou URL da página, que não poderá ser o mesmo do sítio da organização isca e a exibição de um endereço diferente do verdadeiro poderá suscitar suspeitas ao atacado. Para contornar esse empecilho, várias soluções criativas têm sido desenvolvidas pelos atacantes:

- página falsa em *popup*, com carga da página verdadeira em segundo plano, em página cheia. Isso faz com que a página falsa em primeiro plano pareça parte íntegra do sítio da organização isca;

- abertura de *popup*, em tamanho de tela cheia e carga de imagem única contendo inclusive a barra de endereços, botões, barras e menus do programa navegador. Uma outra janela é aberta contendo formulário para captura das informações pessoais do usuário;

- registro e uso de nome de domínio ortograficamente parecido com o nome da organização isca, o que pode passar despercebido ao usuário;

- omissão do nome de domínio e uso de endereço IP na barra de endereços, o que pode confundir o usuário;

- abertura de janela do sítio falso sem a barra de endereços e uso de scripts para criação e exibição de barra de endereços falsa em posição idêntica à janela verdadeira e com conteúdo idêntico; e,

- abertura de janela do sítio falso e sobreposição exata da barra de endereços com caixa de texto contendo o endereço da página verdadeira da organização isca.

Phishing scam associados a cavalos de tróia

Nesta modalidade, a mensagem de correio eletrônico fraudulenta, além de adotar basicamente as mesmas técnicas dissimuladoras para enganar o usuário, traz arquivo anexo contendo código malicioso a ser instalado no computador do usuário destinatário. No conteúdo da mensagem, o apelo é direcionado a que o usuário execute ou clique sobre o arquivo anexo. As razões apresentadas são diversas: instalação de correções de segurança, *download* gratuito de *software* (por exemplo, um antivírus), fotos confidenciais, recadastramento, pornografia, cartões virtuais, oferta de prêmios, formulário de inscrição para sorteios.

Os programas maliciosos, ou cavalos de tróia, poderão ter ações variadas sobre os computadores dos usuários atacados. Coleta e envio de informações pela Internet, pesquisa por informações previamente armazenadas, alteração do arquivo *hosts*, incluindo associações de URLs verdadeiras a endereços IP falsos são alguns dos exemplos de códigos comuns em phishing scam.

Alguns códigos maliciosos mais sofisticados se aproveitam de vulnerabilidades em *software* de correio eletrônico orientado a usuários para disparar a instalação de cavalos de tróia, de maneira automática e silenciosa, independentemente do usuário abrir a mensagem ou executar o clique supostamente necessário para introdução de códigos exógenos perniciosos. Como grande parte dos usuários não realiza as atualizações de segurança disponibilizadas pelos fabricantes, ficam expostos inclusive sem tomar nenhuma ação contributiva.

2.5. Medidas preventivas

Ainda não há como banir a prática de *phishing scam* contra os usuários da Internet e dos serviços das instituições financeiras. Entretanto, as organizações e os usuários podem adotar medidas que ajudem minimizar os efeitos prejudiciais desse incômodo ataque eletrônico.

Políticas consistentes de e-mail

As organizações devem buscar e estabelecer políticas de e-mail com regras bem definidas, especialmente no que se refere ao relacionamento com clientes externos. Essas regras devem ser amplamente divulgadas a todos os clientes ostensiva e periodicamente. A personalização das mensagens direcionadas aos clientes, com informações precisas (incluindo a possibilidade do uso de imagens) sobre eles, pode auxiliar o usuário na identificação das mensagens genuínas da organização. Pode-se também considerar na política, a possibilidade de eliminar o canal correio eletrônico na comunicação organização-cliente, tornando essa prática pública e amplamente divulgada.

Canais de comunicação específicos para consumidores

A disponibilização de canais de comunicação organizacionais para que o usuário esclareça dúvidas, reporte casos de *phishing scam* e submeta mensagens suspeitas pode proporcionar resultados positivos no combate aos *phishing scam* envolvendo instituições financeiras. Endereços específicos de correio e números telefônicos sem tarifa para os usuários são algumas possibilidades de grande utilidade na identificação de mensagens falsas que são direcionadas aos usuários.

Monitoramento da Internet

O monitoramento permanente da Internet em busca de mensagens falsas envolvendo as instituições financeiras também pode ajudar no combate ao *phishing scam*. Mensagens encontradas e rapidamente analisadas, associadas a ações de bloqueios dos endereços receptores de informações pessoais roubadas de usuários e de tráfegos direcionados a sítios fraudulentos podem evitar prejuízos.

Educação dos usuários

O processo de educação dos usuários atuais e potenciais de serviços financeiros eletrônicos é um importante fator de sucesso na redução de ataques de *phishing scam*. Usuários que possam identificar uma mensagem falsa, por perfeita que seja a falsificação, que não sejam facilmente persuadidas através de engenharia social, que internalizem o hábito de atualizar seus sistemas computacionais contra vulnerabilidades de segurança e de instalar ferramentas de proteção às informações armazenadas e processadas no computador, são usuários que dificilmente serão vítimas de mensagens falsas ou de outros tipos de fraudes baseadas em engenharia social. Às organizações cabe assumir seu papel de proporcionar os meios para que os usuários possam desenvolver competências em segurança da informação. Aos usuários cabe a responsabilidade de buscar o aprendizado e aplicá-lo diligentemente.

Parcerias na comunidade Internet

O estabelecimento de parcerias com os atores de infra-estrutura da Internet pode ser fundamental na efetiva realização do combate a *phishing scam*. Pode conferir agilidade aos processos de bloqueio e identificação de sítios e endereços passíveis de mau uso, além de monitoração e bloqueio de tráfego suspeito. Conseqüentemente, pode mitigar ataques potencialmente perigosos e indiretamente, desestimular novas ocorrências.

Uso de filtros antispam

Filtros antispam, especialmente aqueles de nova geração, com recursos mais inteligentes, podem reduzir significativamente a exposição dos usuários a mensagens com intenções duvidosas. Os filtros podem ser instalados tanto nos servidores de correio eletrônico quanto nos equipamentos de usuários.

Ferramentas de proteção

A adoção e instalação de ferramentas, como sistemas antivírus e *firewalls* pessoais, e a manutenção dessas ferramentas permanentemente atualizadas nos computadores dos usuários também é uma medida de bastante utilidade no combate a *phishing scam*, principalmente aqueles associados a cavalos de tróia.

3. CONCLUSÕES

O crescimento das ocorrências de *phishing scam* como ataques eletrônicos direcionados a usuários, especialmente aqueles que se utilizam de sistemas financeiros é preocupação de toda a comunidade Internet. Os ataques têm se tornado mais sofisticados no tempo, tornando-se potencialmente mais eficientes e mais perigosos.

Medidas estruturais nos padrões de comunicação da Internet, que alterem as condições de anonimato e rastreamento real das origens de mensagens, serão implantadas somente em longo prazo, o que as inviabiliza como solução para os problemas atuais de mensagens falsas e ataques de engenharia social contra.

Apesar das organizações usadas atualmente como iscas pelos ataques de *phishing scam* serem os grandes bancos, as tendências apontam a migração brevemente para o uso da imagem de todos os tipos de instituições que lidam com transações sensíveis e financeiras através da Internet, a começar pelos bancos menores [FRAUDWATCH, 2004].

Os governos, legisladores, instituições financeiras, provedores de serviços na Internet, fabricantes de *software* e todas as organizações que usam ou pretendem usar a Internet como canal de negócios devem se empenhar na educação dos usuários em segurança da informação. Esta é a medida que poderá, em médio prazo, contribuir efetivamente para a minimização de *phishing scam* e de outros ataques direcionados a usuários finais.

4. REFERÊNCIAS BIBLIOGRÁFICAS

APWG. Phishing atack trends report – may, 2004. Disponível em <www.antiphishing.org>. Acesso em: jul. 2004.

AUTOR Anônimo; tradução de Edson Furmankiewicz, Joana Figueiredo. *Segurança máxima*. Rio de Janeiro: Campus, 2000.

BOSWORTH, Seymour. *Computer security handbook*. New York: John Wiley & Sons, 4th edition, 2002.

BRASILIANO, Antonio Celso Ribeiro; BLANCO, Lucas. *Manual de planejamento tático e técnico em segurança empresarial*. São Paulo: Sicurezza: 2003.

DIAS, Cláudia. *Segurança e auditoria da tecnologia da informação*. Rio de Janeiro: Axcel Books do Brasil, 2000.

FONTES, Edison. *Vivendo a segurança da informação: orientações práticas para pessoas e organizações*. São Paulo: Sicurezza: 2000.

FRAUDWATCH International. Phishing scams: understanding latest trends. Disponível em <http://www.fraudwatchinternational.com>. Acesso em: jun. 2004.

INFOSEC, HK Government. What is scam?. Disponível em <http://www.infosec.gov.hk/engtext/itpro/sectips/sectips_emailspam.htm>. Acesso em: jul 2004.

McBRIDE, Patrick et alli. *Secure Internet practices*. Boca Raton: Auerbach Publications, 2002.

NBSO, Brasil. Estatísticas dos incidentes reportados ao NBSO. Disponível em <http://www.nbso.nic.br>. Acesso em: jul. 2004.

SEARCHSECURITY, Whatis.com. Phishing. Disponível em <http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci916037,00.html>. Acesso em: jul. 2004.

SEQUEIRA, Dinesh. Intrusion prevention systems: security's silver bullet?. *Business Communications Review*, p. 36-41, mar. 2003. Disponível em <http://www.bcr.com/bcrmag/2003/03/p36.asp>. Acesso em: jun. 2004.

SÊMOLA, Marcos. Gestão da segurança da informação – uma visão executiva. Rio de Janeiro: Elsevier, 2003.

SLEWE, Ton; Hoogenboom, Mark. *Who will rob you on the digital highway?*. Communications of the ACM, vol. 47, n. 5, may. 2004, p.56-60.

STALLINGS, Willian. *Cryptography and network security – principles and practice*. Upper Saddle River: Prentice-Hall, 1998.

SUMMERS, Rita. *Secure computing: threats and safeguards*. New York: McGraw-Hill, 1997.

COOPERAÇÃO POLICIAL INTERNACIONAL NO COMBATE AOS CRIMES CIBERNÉTICOS

Paulo Quintiliano da Silva[1]

[1]Departamento de Polícia Federal, Brasil, Email: quintiliano.pqs@dpf.gov.br

Abstract

Neste artigo são contextualizadas as dificuldades existentes na investigação de crimes cibernéticos com efeitos multinacionais, ressaltando-se a necessidade da cooperação policial internacional. Um projeto de cooperação policial internacional é apresentado, por meio do qual são propostos o estabelecimento e a da adoção de mecanismos céleres, de forma a possibilitar o intercâmbio de informações policiais de forma imediata, bem como a persecução penal de criminosos cibernéticos onde quer que eles estejam.

1. INTRODUÇÃO

O mundo está se convencendo de que a cooperação policial internacional para o combate aos crimes cibernéticos, por meio da adoção de mecanismos céleres, é imprescindível para se levar a bom termo a persecução criminal dessa nova modalidade de ilícitos. Nesse diapasão, apresentamos um projeto de cooperação policial internacional na "V Reunião de Ministros da Justiça das Américas (REMJA V)" da Organização dos Estados Americanos (OEA), realizada em Washington, DC, de 28 a 30 de abril de 2004, o qual será discutido em detalhes na próxima reunião técnica do "Grupo de Peritos Governamentais em Matéria de Delitos Cibernéticos" da OEA. O Conselho da Europa criou o primeiro acordo internacional com o objetivo de atacar essa nova modalidade de crime, intitulado "Convenção de Crimes Cibernéticos", assinado por 26 países em Budapeste, em 23 de novembro de 2001.

Além do Conselho da Europa, várias outras organizações internacionais, como a OEA (Organização dos Estados Americanos), a União Européia, a Europol (*European Police Office*), e as Nações Unidas também estão adotando as suas medidas visando à cooperação policial internacional para o combate aos crimes cibernéticos.

As características dos crimes cibernéticos que mais dificultam o seu combate são os fatos de não existem fronteiras em sua consecução e de que as suas evidências podem se perder definitivamente em pouco tempo. Assim, a mesma ação criminosa pode ter efeito em vários países, de forma simultânea, podendo atingir até milhões de pessoas, como é o caso da disseminação de programas maliciosos, sendo que as evidências que poderiam permitir a identificação e a localização dos autores desses crimes podem se perder definitivamente em pouco tempo [1, 2 e 3].

Dadas as características dessa ação criminosa, em que muitas vezes as suas provas são perdidas definitivamente em poucos meses ou em poucas semanas, para o seu combate efetivo é necessária a cooperação internacional entre os agentes públicos encarregados deste mister, que deve ser feita por meio de grupos organizados e estruturados em cada um dos países, objetivando adotar imediatamente todas as medidas necessárias, sem burocracias.

[1] O autor é Perito Criminal Federal, Chefe do Serviço de Perícias em Informática, Graduado em Ciência da Computação e em Direito, Mestre em Ciência da Computação e Doutor em Reconhecimento de Padrões e Processamento de Imagens.

Dessa forma, em se tratando de crimes cibernéticos, é imprescindível que as ações sejam tomadas de forma extremamente célere, pois, de outra forma, perder-se-iam definitivamente todas as evidências, impossibilitando-se o trabalho da investigação policial.

2. SITUAÇÃO ATUAL

Com base na experiência do Serviço de Perícias em Informática (SEPINF) do Departamento de Polícia Federal em investigações de crimes cibernéticos com efeitos em mais de um país, pode-se constatar que, na grande maioria das vezes, tornam-se inócuos todos os esforços empreendidos pelos policiais, em decorrência da morosidade e, às vezes, da impossibilidade de se conseguirem informações armazenadas em Provedores de Serviços de Internet localizados em outros países.

Considerando-se os procedimentos normais utilizados de forma geral, normalmente são necessárias Cartas Rogatórias para se possibilitar o afastamento dos sigilos telemáticos e a obtenção dos dados das pessoas investigadas junto aos Provedores de Serviços de Internet localizados no exterior. Devido à grande morosidade desses procedimentos, quando os mesmos são concluídos os Provedores de Serviços de Internet responsáveis pela guarda dos dados já liberaram as mídias magnéticas que continham dos dados de interesse, tendo as evidências sido perdidas definitivamente.

Sabe-se que grande parte dos Provedores de Serviços de Internet mantêm as suas cópias com os "logs" dos acessos e demais evidências por, no máximo, 90 (noventa) dias e às vezes por período ainda menor, visto que ainda não existem leis que regulamentam as atividades dos Provedores de Serviços de Internet, obrigando-os a preservarem os dados por mais tempo. Considerando-se a atual forma de trabalho, com a necessidade de Cartas Rogatórias e demais procedimentos, este prazo não é suficiente, o que inviabiliza todo o trabalho de investigação.

Há vários casos trabalhados por este SEPINF, em que criminosos brasileiros, utilizando-se do espaço cibernético, atacaram sítios de entidades governamentais estrangeiras, causando sérios danos. Ressalte-se que o Brasil possui os maiores e mais bem estruturados grupos de criminosos cibernéticos. Quando o processo chega para este Serviço realizar as investigações e as perícias, já se passaram 6 (seis) meses ou mais, não havendo como se chegar à autoria do crime, visto que os dados já se perderam definitivamente.

De forma semelhante, quando precisamos de dados que estão armazenados em Provedores de Serviços de Internet localizados no exterior, para efeito de identificação e localização de suspeitos, em decorrência da grande morosidade dos procedimentos, a solicitação muitas vezes sequer chega a ser feita ao exterior. Isso acontece porque, em se tratando de crimes cibernéticos, não é possível esperar os prazos exigidos pelos procedimentos feitos por meio das Cartas Rogatórias.

Houve outros casos em que foram feitas tentativas junto aos Provedores de Serviços de Internet estrangeiros com representação no Brasil, no sentido de buscar informações de criminosos brasileiros, com base em Ordens Judiciais. A informação recebida foi que os dados estão armazenados em computadores localizados no exterior, e que apenas o Poder Judiciário daquele país poderia autorizar a quebra do sigilo telemático. Essa Ordem Judicial somente poderia ser obtida por meio de uma Carta Rogatória.

3. COOPERAÇÃO POLICIAL INTERNACIONAL PROPOSTA

A proposta brasileira consiste no estabelecimento de cooperação hemisférica, por meio da adoção de mecanismos ágeis no combate aos delitos cibernéticos, especialmente aos que têm repercussão internacional. Os mecanismos propostos procuram evitar, sempre que possível, todos os procedimentos burocráticos e morosos, incompatíveis com a velocidade que experimentam os crimes cibernéticos e com a agilidade dos criminosos do espaço cibernético.

No âmbito desta proposta, está sendo considerada a necessidade da "nacionalização das evidências" produzidas no exterior. Sempre que houver convênios bilaterais ou multilaterais entre os países participantes da cooperação, a "nacionalização das evidências" deve ser feita por meio dos

mesmos. Na ausência dos convênios ou em casos de dificuldades na sua utilização, serão utilizados os procedimentos descritos nesta proposta para efeito da "nacionalização das evidências".

A cooperação internacional para o combate aos crimes cibernéticos, proposta pelo Brasil, tem como pressuposto a existência de Grupos Técnicos formados por policiais especializados na investigação desses crimes, estruturados e organizados em cada um dos países participantes. Esta cooperação pode e deve se estender aos demais países não membros da OEA, de forma que a mesma se torne universal e possa alcançar todas as localidades conectadas na Internet. As ações e mecanismos propostos serão adotados principalmente por esses Grupos Técnicos de cada país, da forma mais ágil possível, e com o mínimo de formalidade e delongas.

Sabe-se da existência da "Rede de Emergência 24 horas/7dias", organizada e administrada pelo G8, da qual o Brasil é membro, sendo que o ponto de contato brasileiro é o Serviço de Perícias em Informática (SEPINF) da Polícia Federal. Esta Rede, também conhecida como "G8 24/7 *Computer Crime Network*", já possui pontos de contatos e está estruturada em diversos países, e pode e deve ser utilizada na implantação de nossa proposta, com as devidas estruturações e adequações em alguns de seus pontos de contatos, quando for o caso. Para tanto, é necessária a criação de grupos técnicos especializados em investigação de crimes cibernéticos em todos os países membros da OEA, os quais funcionarão como os pontos de contatos da Rede. É importante que os membros desses grupos sejam policiais com formação superior em Ciência da Computação ou com bastante conhecimento e experiência em investigação de crimes cibernéticos. O ideal é que esses grupos sejam criados em todos os países conectados na Internet, de forma que a cooperação seja universal e feita por todos os países, de maneira uniforme.

Certamente haverá a necessidade de uma discussão mais detalhada do projeto pelo "Grupo de Peritos Governamentais em Matéria de Delito Cibernético", em reunião específica desse grupo ou em reunião conjunta com o grupo das "Autoridades Centrais e Outros Peritos em Assistência Jurídica Mútua em Matéria Penal".

Essa proposta de cooperação considera duas vertentes distintas: (1) inversão da persecução penal e (2) fornecimento de evidências para serem utilizadas em processos penais de outros países.

3.1. Inversão da persecução penal

Esta vertente se aplica nos casos em que indivíduos residentes no país A, agindo dentro do território de seu próprio país, cometem crimes que surtem efeitos no país B, e em outros. Esta vertente da cooperação proposta dever cumprir os seguintes passos:

1) O Grupo Técnico do país B, tomando conhecimento da ocorrência do delito cibernético, entra em contato com o Grupo Técnico do país A, solicitando a cooperação e lhe encaminhando todas as evidências comprobatórias da ocorrência do fato. Esses pedidos têm que ser feitos da forma mais rápida possível, por telefone e/ou por e-mail, garantindo-se a máxima celeridade possível.

2) Ao receber a solicitação de cooperação, o Grupo Técnico do país A, com base nas evidências recebidas, imediatamente assume o comando das investigações, iniciando procedimento investigatório, produzindo-se novas evidências a partir de suas próprias investigações, na forma de laudos periciais e relatórios técnicos. Dessa forma, as evidências produzidas por investigações realizadas no exterior são "nacionalizadas" por meio das investigações feitas no próprio país onde residem os suspeitos, com base nas "evidências estrangeiras", gerando-se "evidências nacionais", na forma de laudos periciais e relatórios técnicos, com o necessário valor legal.

3) O Grupo Técnico do país A, após a realização de investigações preliminares e da obtenção das necessárias evidências, solicita o afastamento do sigilo telemático e a interceptação telemática ao Poder Judiciário, obtendo as necessárias Ordens Judiciais.

4) Com base nas Ordens Judiciais para o afastamento do sigilo telemático e para a interceptação telemática, os policiais do Grupo Técnico do país A obtêm junto aos provedores de serviços de Internet todas as informações necessárias para se chegar à autoria dos crimes. Com base nessas informações, novos exames periciais são realizados, produzindo-se novas "evidências nacionais", na forma de laudos periciais, com o objetivo de identificar e localizar os autores dos crimes cibernéticos.

5) Após a identificação e a localização dos autores dos crimes, são solicitadas Ordens Judiciais para busca e apreensão de material de informática e das demais evidências nos endereços dos investigados.

6) Como base no material apreendido, serão produzidas novas evidências, principalmente na forma de laudos periciais, consolidando a convicção dos investigadores, no sentido de se solicitar novas Ordens Judiciais para a prisão dos investigados.

Dessa forma, o processo investigativo de cada país é constituído e instruído com base em todas as evidências obtidas, a partir da solicitação de apoio e das "evidências" estrangeiras, com a maior celeridade possível, evitando-se burocracias desnecessárias e a possibilidade da perda das evidências. Assim, nesse caso a idéia é proceder a inversão da persecução penal, de forma que o país onde residem os criminosos cibernéticos se torne o responsável por toda a persecução penal, com base no pedido de cooperação e nas evidências recebidas do exterior. Após a sua conclusão dos procedimentos investigativos, o processo é encaminhado ao Poder Judiciário e Ministério Público, para continuidade da persecução penal.

3.2. Fornecimento de evidências para outros países.

Esta vertente se aplica nos casos em que indivíduos residentes no país A, agindo dentro do território de seu país, cometem crimes que surtem efeito dentro de seu próprio país, mas as evidências comprobatórias da ocorrência dos crimes estão armazenadas em computadores localizados no país B, e em outros. Esta vertente da cooperação proposta cumpre os seguintes passos:

1) O Grupo Técnico do país A, tomando conhecimento da ocorrência do delito cibernético, entra em contato com o Grupo Técnico do país B, solicitando a cooperação e encaminhando-lhe todas as evidências comprobatórias da ocorrência do fato. Esses pedidos têm que ser feitos da forma mais rápida possível, por telefone e/ou por e-mail, garantindo-se a máxima celeridade possível.

2) Ao receber a solicitação de cooperação, o Grupo Técnico do país B, com base nas evidências recebidas, realiza investigações preliminares e/ou exames periciais no material recebido, produzindo-se "evidências nacionais", na forma de laudos periciais e relatórios técnicos. Dessa forma, ocorre o procedimento de "nacionalização" das evidências recebidas.

3) Com base nas "evidências nacionais" produzidas, o Grupo Técnico do país B, solicita o afastamento do sigilo telemático e a interceptação telemática ao Poder Judiciário, obtendo as necessárias Ordens Judiciais. Com base nessas Ordens, são obtidas junto aos provedores de serviços de Internet todas as informações necessárias para se chegar à autoria dos crimes, bem como à localização dos suspeitos. A partir dessas informações, novos exames periciais são realizados, produzindo-se novas "evidências nacionais", na forma de laudos periciais, com o objetivo de identificar e localizar os autores dos crimes cibernéticos.

4) Todas essas evidências são encaminhadas ao Grupo Técnico do país A, para serem utilizadas em persecução penal a ser realizada naquele país, onde haverá procedimento semelhante de "nacionalização dessas evidências".

4. PREMISSAS BÁSICAS

Para que a cooperação policial internacional aqui proposta funcione adequadamente, é necessário que os países partícipes observem os aspectos abaixo relacionados.

1) Torna-se necessário que os pontos de contatos de todos os países, representados pelos Grupos Técnicos, estejam estruturados com as condições mínimas necessárias, em termos de equipamentos e softwares disponíveis, bem como de pessoal qualificado e treinado, de forma que o atendimento das solicitações de apoio possa ser feito com a máxima agilidade e da melhor forma possível.

2) Torna-se necessário o compromisso de todos os países no sentido de envidarem esforços, efetuando o apoio internacional solicitado, com a maior celeridade possível.

3) Também é necessária uma maior aproximação das Forças Policiais com o Ministério Público e com o Poder Judiciário, de forma que todas essas instituições envolvidas no combate aos crimes cibernéticos entendam bem as características peculiares que têm esses novos crimes. Essa aproximação e esse entendimento evitarão que se perca tempo internamente dentro de cada país.

4) É necessário que os Grupos Técnicos sempre tenham acesso a programas específicos de treinamento, de forma que os investigadores tenham todos os conhecimentos técnicos e científicos necessários para realizarem investigações no espaço cibernético. Nesses treinamentos, além da parte conceitual, há a necessidade de módulos específicos para a utilização de certas ferramentas forenses, necessárias em certos tipos de investigação.

5) É recomendável que sejam estabelecidos padrões de atuação a serem observados por todos os Grupos Técnicos dos países, com o objetivo de facilitar e de agilizar os procedimentos a serem adotados.

5. CONVENÇÃO DE CRIMES CIBERNÉTICOS DO CONSELHO DA EUROPA

A Convenção de Crimes Cibernéticos do Conselho da Europa foi aberta para assinatura, na cidade de Budapeste, em 23 de novembro de 2001. Atualmente já conta com as assinaturas de 38 países, sendo que 6 desses já fizeram a ratificação. A convenção entrou em operação em 01/07/2004, após a ratificação dos cinco primeiros países, conforme estabelece o item 3 do artigo 36 da Convenção.

Esta Convenção estabelece uma série de exigências que os países devem adotar, no sentido de adequar as suas legislações, de forma a tipificar como crimes várias condutas ilícitas praticadas por meio da Internet. O Serviço de Perícias em Informática da Polícia Federal está trabalhando na elaboração de minuta de Projeto de Lei para o atendimento das exigências da Convenção de Crimes Cibernéticos, em que estão sendo tipificadas como crimes todas as condutas ilícitas relacionadas na Convenção. Este trabalho está sendo feito juntamente com a Câmara dos Deputados. A Convenção também estabelece exigências em termos de legislação processual, que também está sendo prevista nessa minuta de Projeto de Lei.

A Convenção também se preocupa com a cooperação internacional visando ao combate aos crimes cibernéticos, estabelece critérios para a cooperação entre os países, bem como estabelece princípios gerais para a assistência legal mútua. Estabelece que os países membros da Convenção devem aderir à Rede 24/7 do G8, bem como designar os seus pontos de contatos a essa rede. O Brasil já faz parte da Rede 24/7, sendo que o ponto de contato brasileiro é o Serviço de Perícias em Informática da Polícia Federal.

O Serviço de Perícias em Informática da Polícia Federal também elaborou minuta de Projeto de Lei para regulamentar as atividades dos Provedores de Serviços de Internet brasileiros. Os "Cyber Cafè" são tratados como Provedores de Serviços de Internet, e deles é exigido, dentre outras coisas, que mantenham cadastro de todos os usuários, de forma que os mesmos possam ser identificados quando necessário..

6. CONCLUSÕES

Os crimes cibernéticos estão experimentando um grande crescimento nos últimos anos. Se tais atividades criminosas não forem combatidas com o devido vigor, pode haver grande prejuízo nas atividades sérias que vêm sendo conduzidas por meio do espaço cibernético, tanto as atividades governamentais, como as comerciais e as científicas.

Nos casos em que as atividades criminosas ultrapassam as fronteiras do país, é imprescindível que haja a cooperação internacional, por meio dos grupos de cooperação formados pelos órgãos governamentais responsáveis, de modo a ser possível enfrentarmos com eficácia essa nova face do crime que o século XXI nos apresenta. É importante que esses grupos atuem com eficiência e eficácia, evitando-se maiores burocracias, buscando-se a necessária celeridade exigida por esse tipo de crime [1, 2 e 3].

Em se tratando de crimes cibernéticos praticados a partir de ou com efeitos em vários países, em grande parte das vezes, um país atuando isoladamente não consegue fazer praticamente nada em termos de investigação, visto que as evidências que poderão comprovar a autoria do crime estão armazenadas fora do país, sob proteção de sigilo. Além disso, os criminosos também residem no exterior, longe do alcance das leis e do poder coercitivo do país ofendido. Assim, para se lograr êxito no combate a esses crimes, é imprescindível que haja o estabelecimento de uma cooperação internacional, de forma compromissada e célere.

Entendemos que, com a criação e a implantação dos mecanismos propostos neste projeto nos diversos países membros da OEA e em outros se possível, será viável a investigação dos crimes cibernéticos com repercussão internacional, de forma eficaz.

7. REFERÊNCIAS BIBLIOGRÁFICAS

[1] Paulo Quintiliano da Silva, 2003, "Crimes Cibernéticos no Contexto Internacional", **In**: Anais do XIII Congresso Mundial de Criminologia, Rio de Janeiro-RJ, Brasil.

[2] Paulo Quintiliano da Silva, 2003, "Perícias em Crimes Cibernéticos", **In**: Anais do XVII Congresso Nacional de Criminalística, Londrina-PR, Brasil.

[3] Paulo Quintiliano da Silva, 2004, "Crimes Cibernéticos e Seus Efeitos Multinacionais", **In**: Revista Perícia Federal, Brasil.

[4] _____, 2001, "Convention on Cybercrime", Council of Europe.

RECONHECIMENTO FACIAL APLICADO À PERÍCIA CRIMINAL

Paulo Quintiliano da Silva[1], Antônio Nuno de Castro Santa Rosa[2]

[1]Departamento de Polícia Federal, Brasil, Email: quintiliano.pqs@dpf.gov.br

[2]Universidade de Brasília, Brasil, Email: nunos@unb.br

Abstract

Neste artigo é apresentado um breve histórico do reconhecimento facial. São também abordados alguns aspectos psicológicos do assunto e modelos propostos para o entendimento da percepção facial. Um modelo de reconhecimento facial automatizado, baseado nas eigenfaces, é proposto e apresentado em detalhes. São apresentadas aplicações do algoritmo de reconhecimento facial para a perícia criminal, especialmente para o reconhecimento de pessoas em cenas de crimes. Com a finalidade de reconhecer pessoas com a face semi-oclusa, com o uso de máscaras ou outro artefato, normalmente em cenas de crimes, os conceitos das eigenfaces são estendidos para eigeneyes, eigenmouth e eigennose, com a finalidade de reconhecer as pessoas nessa situação adversa.

1. INTRODUÇÃO

O reconhecimento de faces conhecidas tem um papel fundamental nas relações sociais das pessoas, apresentando-se como uma função corriqueira para o cérebro humano, contudo extremamente importante para as atividades mais simples e cotidianas, visto que o relacionamento das pessoas com as outras está baseado no reconhecimento facial. Normalmente, as pessoas só estabelecem uma interação com as outras se estas forem identificadas como exatamente os indivíduos com quem se quer interagir; e esta identificação usualmente se dá por meio do reconhecimento facial. As pessoas normalmente conseguem reconhecer um grande número de faces, sendo que este processamento extremamente complexo se dá de forma bastante natural.

Dada a natureza muito particular do reconhecimento facial, há pesquisadores que afirmam que o cérebro humano possui uma região específica para este tipo de reconhecimento. Os psicólogos e médicos que pesquisam áreas correlatas com a neurologia se interessam muito em entender o mecanismo utilizado pelo cérebro humano para o reconhecimento facial.

2. HISTÓRICO

A literatura constata o início de esforços em pesquisas tratando de reconhecimento de faces desde o século XIX. Em 1878, o cientista inglês Sir Francis Galton apresentou um artigo no Instituto de Antropologia Britânico, em que ele descreveu as suas pesquisas envolvendo a combinação de fotos de pessoas, por meio da sobreposição de imagens de faces, umas sobre as outras, sendo que ele concluiu que se poderia chegar à foto que apresentaria as suas características típicas, reduzindo ou eliminando as variações existentes. O método de Galton propôs o alinhamento das fotos de faces das pessoas, em função de suas características marcantes, como a região dos olhos, e sobrepondo-as umas sobre as outras. Galton imaginou uma série de aplicações úteis para a sua *Composite Portraiture* (Combinação de Fotos), como a obtenção de uma melhor idéia da aparência de figuras históricas, pela combinação de quadros de diversos artistas, em que os diversos estilos artísticos deveriam desaparecer e a verdadeira aparência da personagem se sobressair, e outros, conforme se pode observar na Figura 01.

Em 25 de maio de 1888, no instituto de identificação de pessoas, do Instituto Royal Britânico, Galton relata a sua grande dificuldade de descrever verbalmente ou por escrito as semelhanças hereditárias ou não entre as pessoas, os tipos de faces e características de cada pessoa. Em decorrência destas dificuldades, ele cometeu grandes enganos em seu trabalho e, a partir daí, começou a fazer interessantes experimentos, procurando caracterizar e identificar as pessoas por meio de seus caracteres físicos. Assim, Galton desenvolveu o que ele próprio chamou de "mechanical selector", baseado em biometria, que permitia a comparação de perfis de medidas da face [02, 05, 06 e 12]. Ele também usou outras quatro medidas primárias: tamanho da cabeça, profundidade da cabeça, tamanho dos pés e tamanho dos dedos médios da mão e do pé.

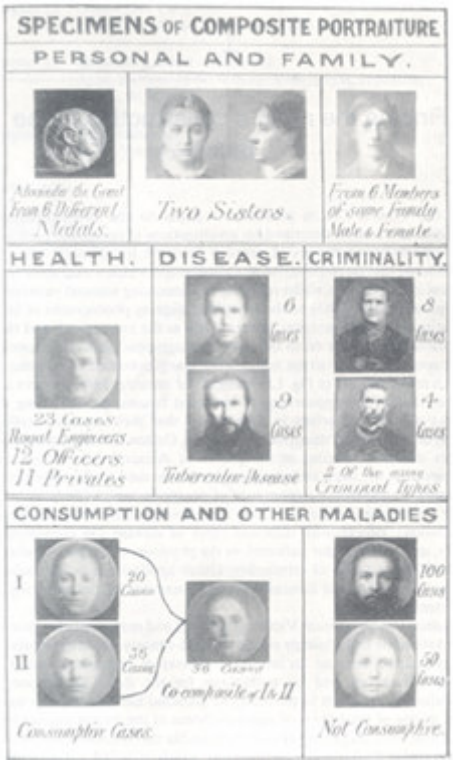


Figura 01 - Composição de Fotos de Galton.

A idéia de comparação de medidas introduzida por Galton é utilizada em pesquisas atuais na Ciência da Computação, em que são extraídas características biométricas da imagem da face para serem comparadas com as medidas de outras faces, procurando-se o reconhecimento facial.

Alguns pesquisadores desenvolveram modelos baseados nas características geométricas da face humana, em que esses dados são calculados com base na geometria facial representada na imagem das faces. Foram utilizados até 100 pontos de controle ou vetores caracterizando as particularidades das faces. Usaram-se, como parâmetros de comparação, as medidas das partes da face, a distância entre cada um dos componentes da face com os demais.

A verificação de reconhecimento de pessoas com base na aparência facial é uma área de grande interesse da Visão Computacional, tendo sido objeto de muita pesquisa e desenvolvimento.

A biometria facial, usada desde os tempos de Galton, é uma técnica que vem se desenvolvendo muito nos últimos anos, apresentando-se como uma ferramenta bastante útil para o desenvolvimento das técnicas de reconhecimento facial.

3. ASPECTOS PSICOLÓGICOS DO RECONHECIMENTO FACIAL

De acordo com a abordagem psicológica, existem dois níveis do reconhecimento da face: reconhecimento em nível de entrada e o reconhecimento do em nível subordinado. No reconhecimento em nível de entrada, todas as faces são percebidas como uma única categoria de "face"; e no reconhecimento em nível subordinado, as faces individuais são distinguidas por distinções mais finas. Há muitos experimentos feitos por psicólogos procurando descobrir a extensão das habilidades humanas em reconhecer faces em condições desfavoráveis de iluminação, com fotos de cabeça para baixo ou em posição invertida em 90º, ou com expressões faciais variadas, como surpresa, sorriso, irritação e outras [01 e 13].

Observações de neuropsicólogos e experimentos de psicólogos concluem que o cérebro humano processa o reconhecimento facial por meio de canais de processamento de informações específicos para esta finalidade. Devido à natureza extremamente particular da atividade, esses cientistas afirmam

que há fortes evidências de que as expressões faciais e o reconhecimento facial são processados por caminhos diferentes de processamento e também são diferentes os caminhos que processam o reconhecimento facial de pessoas familiares e de pessoa estranhas. Tudo isto foi constatado por meio de experimentos, em que vários pacientes foram estudados, apresentando a eles situações diversas de reconhecimento facial, como de pessoas estranhas, pessoas conhecidas, com ou sem expressões faciais, com fotos apresentadas em posições diferentes da vertical. Constatou-se que algumas pessoas têm mais facilidade de reconhecer pessoas estranhas, que só foram vistas uma ou poucas vezes. As observações neuropsicológicas foram baseadas em resultados de exames de neurologia. Algumas das células apontadas como responsáveis pelo Reconhecimento Facial apresentam especializações para expressões emocionais, outras apresentam especializações diferentes.

Como há grande número de cientistas que afirmam que o cérebro possui uma área especializada para o Reconhecimento Facial, também há evidências relatadas por cientistas de que algumas pessoas já nascem com grande predisposição e facilidade para o reconhecimento de padrões como a face humana. A despeito de haver observações com comprovado valor científico demonstrando que as faces são objetos especiais no mundo visual das pessoas, demandando uma parte do cérebro exclusivamente para o seu reconhecimento, ainda não há comprovação de que o processo de Reconhecimento Facial difere fundamentalmente dos processos utilizados no reconhecimento de outros tipos de objetos.

Os psicólogos e médicos que pesquisam áreas correlatas com a neurologia se interessam muito em entender o mecanismo utilizado pelo cérebro humano para o reconhecimento facial. Também para os pesquisadores da Visão Computacional e Processamento de Imagens é muito importante conhecer o mecanismo utilizado pelo cérebro humano para o reconhecimento facial, pois poder-se-ia tentar utilizar mecanismos semelhantes no reconhecimento facial feito por computador, já que trata-se esta matéria de um projeto muito complexo.

4. MODELOS PSICOLÓGICOS DE RECONHECIMENTO FACIAL

Os cientistas Hay e Young [04] desenvolveram pesquisas procurando explicar o reconhecimento de faces familiares baseado em uma unidade que eles descobriram e denominaram de unidades de reconhecimento facial - URF. Esses cientistas afirmam que a URF atinge um limiar máximo de excitação quando a pessoa vê uma face conhecida. O cérebro humano ao receber o estímulo proveniente do fato de ver uma face, codifica esta face usando uma representação bastante completa e passa esta informação para a URF, que, por sua vez, experimenta um certo grau de excitação. Esse grau de excitação varia proporcionalmente ao grau de certeza de reconhecimento da face em tela, por exemplo, de 0 a 1, sendo que se a excitação for próxima de 0 a face é desconhecida, e se for próxima de 1 a face foi reconhecida.

Os cientistas Cantor e Mischel [03] desenvolveram pesquisas procurando sistematizar o processo utilizado pelo cérebro para o reconhecimento de objetos, encontrando um modelo com três situações possíveis para mostrar quando um determinado objeto foi identificado, denominado-as de clássica, exemplificativa e prototipagem. No modelo clássico, o observador utiliza uma lista de atributos necessários para a descrição do objeto visual, sendo que o reconhecimento ocorre quando o observador fica satisfeito com o estímulo visual recebido em função de todos os atributos necessários ao reconhecimento. No modelo exemplificativo, o observador utiliza um modelo de exemplos de coleções de ocorrências de objetos visuais, sendo que o estímulo visual é verificado com a base nas semelhanças de exemplos conhecidos. No modelo de prototipagem, o observador usa um modelo de protótipo que é uma imagem-resumo ou um conjunto de características de um objeto visual, sendo que o estímulo visual é confrontado com a base nas semelhanças do protótipo utilizado.

Outros pesquisadores concluíram que o Reconhecimento Facial é desenvolvido naturalmente pelo cérebro humano em termos de um modelo de faces. Este protótipo é criado a partir de todas as faces vistas pela pessoa, e cada nova face observada é codificada e acrescentada ao modelo. Todas as características das faces são concebidas, estendendo-se em todas as direções do modelo, representando a origem do depósito de características faciais. Uma face bastante conhecida, com semelhanças fortes com relação ao modelo, pode ser localizada rapidamente perto da origem. Por outro lado, se a face considerada for muito comum ou de difícil reconhecimento, o espaço próximo da

origem estará muito cheio com informações de outras faces mais conhecidas, e as informações desta face pouco conhecida estarão no fim do modelo, cujo acesso é mais difícil. Constataram-se evidências nas pesquisas feitas por cientistas concluindo que o reconhecimento de faces conhecidas demanda uma quantidade menor de memória, comparando-se com o reconhecimento de faces desconhecidas.

5. RECONHECIMENTO FACIAL AUTOMÁTICO

O Reconhecimento Facial Automático consiste na verificação ou identificação de uma pessoa por meio da comparação de uma face com uma única face (uma para uma) ou com um banco de dados de faces (uma para muitas). O Reconhecimento Facial é executado em nível subordinado. Nesta fase, uma face nova é comparada com faces conhecidas armazenados em um banco de dados, sendo então classificada como sendo a face de um indivíduo conhecido ou como uma face desconhecida.

Para que o Reconhecimento Facial Automático possa ser levado a efeito, é necessário que haja uma fase anterior - a Detecção Facial Automática - que tem por objetivo localizar uma face no cenário complexo proposto, recortar a imagem da face, eliminar o fundo remanescente e apresentar uma "janela" contendo a face para o modelo de Reconhecimento Facial Automático. O Reconhecimento Facial vem se tornando uma área de pesquisa que tem atraído muito interesse da comunidade científica, tendo numerosas pesquisas e aplicações nos últimos anos.

Pode-se considerar que a atividade de reconhecimento de faces (automática ou natural) possui três etapas distintas: Representação Facial, Detecção Facial e Reconhecimento Facial. A Representação Facial se constitui na modelagem da face, na tradução da face em códigos que possam ser entendidos e usados pelos algoritmos de Detecção Facial e Reconhecimento Facial. Um registro armazenado num banco de dados qualquer pode ser representado facilmente por sua chave primária, mas a representação de uma imagem de face não é trivial, demandando algoritmos complexos para possibilitar uma boa representação. O modo de representar uma face determina os algoritmos sucessivos de detecção e identificação. Para o reconhecimento em nível de entrada, uma categoria de faces deveria ser caracterizada por propriedades genéricas de todas as faces; e para o reconhecimento em nível subordinado, características detalhadas de olhos, nariz e boca têm que ser consideradas em cada face individual. Existem pesquisas no desenvolvimento de várias técnicas de representação facial, que podem ser enquadradas em três categorias distintas: *Template-based*, *Feature-based* e *Appearance-based*.

O método *Template-based* de Representação Facial possui duas versões, a primeira – e mais simples – se propõe a representar as faces por meio de uma matriz bidimensional com valores representando as bordas da elipse facial e de todos os órgãos da face. A segunda versão deste método – mais completa – apresenta múltiplos *templates* na representação das faces, sob diversos ângulos e pontos de vista. Outra abordagem importante é empregar um conjunto de modelos de características faciais menores, correspondente aos olhos, nariz e boca, para um único ponto de vista. A vantagem mais atraente deste modelo é a sua simplicidade, porém tem a desvantagem de necessitar grande quantidade de memória e de ser um algoritmo de comparação ineficiente.

O método *Feature-based* considera as posições e tamanhos dos órgãos faciais, como olhos, nariz, boca, sobrancelhas, etc., na representação das faces. Este método consome bem menos recursos computacionais do que o *template-based*, possibilitando maior velocidade de processamento, podendo-se obter bons desempenhos com banco de dados de faces em escalas variadas. O método de comparação baseado nas características geométricas usa um banco de dados com um modelo para cada face (tamanho e posição de olhos, boca, esboço de cabeça, e relações entre estas características). Para cada imagem são calculadas todas as distâncias entre os órgãos da face. A meta é adquirir uma correspondência do tipo "um para um" entre as características da face questionada e as características das faces armazenadas em num banco de dados. As características extraídas por gradientes verticais são úteis para a detecção do topo da cabeça, olhos, base de nariz e boca. Os gradientes horizontais são úteis para detecção dos limites laterais da face e do nariz. Para cada face deve ser calculado um vetor de características e então o reconhecimento é executado com um classificador vizinho mais próximo.

O método *Appearance-based* se propõe projetar as imagens de faces num subespaço linear de baixa dimensão, obtendo-se, a partir desta projeção, a representação das faces. O espaço das *eigenfaces* é uma aplicação deste método, sendo construído com base na PCA – *Principal Component*

Analysis, a partir da projeção das imagens do conjunto de treinamento no espaço de faces (de baixa dimensão). Nesta dissertação, o conceito de *eigenfaces* foi expandido para as *eigenfeatures*, como *eigeneyes*, *eigenmouth* e *eigennose*, com o objetivo melhorar a eficácia dos algoritmos quando trabalhando com imagens semi-oclusas.

A detecção facial consiste em, dada uma imagem de um cenário complexo, localizar uma face, recortá-la para ser apresentada ao algoritmo de Reconhecimento Facial. Alguns métodos utilizam a busca de uma forma elíptica, outros procuram a textura da cor de pele e há os que procuram pelos órgãos da face, como olhos, boca, nariz, etc. A detecção facial é executada em nível de entrada.

O Reconhecimento Facial Automático consiste na constatação da identidade de uma pessoa por meio da comparação de uma face com uma única face - Verificação Facial - (uma para uma) ou com um banco de dados de faces – Identificação Facial - (uma para muitas). O Reconhecimento Facial é executado em nível subordinado. As faces apresentadas para efeito de reconhecimento são comparadas com as faces conhecidas armazenados em um banco de dados, sendo então classificadas como sendo a face de um indivíduo conhecido ou como uma face desconhecida.

Esta pesquisa foi desenvolvida com base no método de representação de faces *appearance-based*, usando-se como suporte os *autovetores* das imagens e seus respectivos *autovalores*. Este método utiliza a KLT (*Karhunen-Loève Transform*), decompondo as imagens de faces em um pequeno conjunto de características particulares das imagens, chamado *eigenfaces*. O reconhecimento é executado por meio da projeção das faces novas (faces questionadas) em um espaço linear de faces de baixa dimensão, criado a partir das *eigenfaces* e calculando-se a distância euclidiana existente entre cada face questionada e o espaço de faces das classes, construído com base nas faces conhecidas.

Na implementação deste modelo, foram obtidos altos índices de reconhecimento, sendo que o modelo se mostrou bastante robusto ao trabalhar com imagens obtidas em condições favoráveis de iluminação, mesmo com expressões faciais diversas e utilização de óculos, sendo, entretanto, sensível para se trabalhar com imagens obtidas em condições extravagantes de iluminação e em diferentes escalas. Para estes casos, foram desenvolvidas técnicas para diminuir os efeitos da iluminação inadequada, que foram chamadas de simetrização. A aplicação destas técnicas melhorou significativamente o desempenho do modelo quando as imagens trabalhadas tiverem sido obtidas em condições inadequadas de iluminação, especialmente com iluminações laterais.

A maior parte dos esforços em pesquisas relativas ao Reconhecimento Facial enfocou reconhecimento em nível subordinado, ficando o reconhecimento em nível de entrada em segundo plano. Ressalte-se que as pesquisas aqui apresentadas enfocaram com maior interesse o reconhecimento em nível subordinado. A detecção facial é classificada em nível de entrada, enquanto que o reconhecimento facial é classificado em nível subordinado.

O desempenho do reconhecimento de faces pode ser comprometido por vários fatores, dentre eles são destacados os principais: iluminação inadequada, baixa resolução da imagem, escala, posição da face, disfarce e expressão facial.

6. MODELO DE RECONHECIMENTO FACIAL AUTOMÁTICO PROPOSTO

Neste tópico será descrito o modelo de reconhecimento automático desenvolvido. Na construção dos espaços de imagem e de faces, parte-se de um conjunto de *M* imagens de faces, as mesmas obtidas a partir do algoritmo de Detecção Facial, identificadas como $\Gamma_i (i = 1,...,M)$ e referenciadas como o conjunto de imagens de treinamento. Estas imagens são utilizadas para o treinamento do modelo e para a verificação de seu desempenho. Essas imagens são matrizes quadradas de *NxN*, portanto tendo cada imagem N^2 *pixels*, em que N=128.

Preliminarmente, todas essas M imagens são convertidas em vetores coluna, passando a terem a dimensão $N^2 x1$, com os mesmos N^2 pixels. Essa conversão se dá tomando cada uma das linhas e concatenando-as, uma em seguida à outra, de forma a se construir o vetor coluna, da seguinte forma:

$$\Gamma_{i,1} = \Gamma'_{j,k} \;\; (i = 1,...,N^2;\; j,k = 1,...,N) \qquad (1)$$

Calcula-se, então, a face média Ψ de todo o conjunto de imagens, somando-se todas as imagens e dividindo-se o resultado pela quantidade de imagens, da seguinte forma:

$$\Psi = \frac{1}{M}\sum_{i=1}^{M}\Gamma_i \,. \tag{2}$$

Uma vez calculada a face média Ψ (também com N^2 *pixels* e dimensão $N^2 x1$), é montado um novo conjunto de imagens Φ_i, obtido a partir da diferença entre cada uma das imagens do conjunto de treinamento e a face média.

Assim, cada uma das imagens Φ_i se distancia (diferencia-se) da face média da distribuição, e esta distância é calculada subtraindo-se a face média de cada face, chegando-se a um novo espaço de imagens, calculado da seguinte forma:

$$\Phi_i = \Gamma_i - \Psi(i = 1,...,M) \tag{3}$$

A partir do novo conjunto das *M* imagens Φ_i (todas com dimensão $N^2 x1$, com N^2 *pixels*, portanto), é montada a matriz *A*, de dimensão $(N^2 xM)$, tomando-se cada um dos *M* vetores Φ_i e colocando-os em cada coluna da matriz A, da seguinte forma:

$$A_{i,j} = \Phi_{j;i,1} \tag{4}$$

A partir da matriz *A*, a matriz de covariância C teria que ser montada, por meio de produto externo, com dimensão $N^2 xN^2$, da seguinte forma:

$$C = AA^T \tag{5}$$

Foi escolhida a alternativa de montar a matriz de covariância L, por meio de produto interno, com dimensão *MxM*, prescindindo-se da montagem da matriz C, para efeito de melhoria de performance. O cálculo da matriz L se dá da seguinte forma:

$$L = A^T A \tag{6}$$

Será mostrada, então, a equivalência entre os *autovetores* de L e os de C. Sejam as matrizes $A_{(N^2 xM)}$ e $A^T{}_{(MxN^2)}$, sendo $N^2 \geq M$. Então, temos:

$$\begin{vmatrix} -\lambda I_{N^2} & -A \\ A^T & I_M \end{vmatrix} = (-\lambda)^{N^2-M} \left|A^T A - \lambda I_M\right| = \left|AA^T - \lambda I_{N^2}\right| \tag{7}$$

Então, os N^2 *autovalores* de AA^T são iguais aos *M autovalores* de $A^T A$, acrescidos dos $N^2 - M$ *autovalores* iguais a zero. Será apresentado a seguir um teorema da Álgebra Linear que descreve bem o relacionamento entre os *autovetores* de AA^T e de $A^T A$.

Teorema: Para as matrizes $A_{(N^2 xM)}$ e $A^T{}_{(MxN^2)}$, os *autovalores* diferentes de zero de AA^T e $A^T A$ são os mesmos e têm a mesma multiplicidade. Se x é um *autovetor* não trivial de AA^T para um *autovalor* $\lambda \neq 0$, então $y = A^T x$ é um *autovetor* não trivial de $A^T A$.

Prova: A primeira parte obtém-se a partir de (21). Para a segunda parte, substituindo-se $y = A^T x$ na equação $(A^T(AA^T x) = \lambda A^T x)$ chega-se a $(A^T Ay = \lambda y)$. O vetor *x* não é trivial se $x \neq 0$. Desde que $(Ay = AA^T x = \lambda x \neq 0)$, conclui-se também que $y \neq 0$.

Então, os *autovetores* da matriz de covariância L são calculados. Esses cálculos são feitos da forma como se segue. Seja a matriz quadrada L, de dimensão (*MxM*), os *autovalores* λ de L são as raízes da equação:

$$\left|L - \lambda I\right| = 0 \tag{8}$$

Os autovetores, por sua vez, são os vetores x_i não nulos que satisfazem a seguinte equação:

$$\left(L - \lambda_i I\right) x_i = 0 \tag{9}$$

Como, pelo Teorema anteriormente apresentado, os *autovetores* de C são equivalentes aos *autovetores* de L, os *autovetores* de C são calculados a partir dos *autovetores* de L. Este cálculo pode

ser feito a partir do somatório da combinação linear das matrizes do espaço Φ_k com os M elementos dos M autovetores de L, conforme apresentado na seguinte equação:

$$u_l = \sum_{k=1}^{M} v_{lk} \Phi_k, \ (l = 1,...,M) \tag{10}$$

Como, considerando-se as matrizes $A_{(N^2 xM)}$ e $V_{(MxM)}$, em que A contém as M imagens do espaço Φ_k e V contém os M autovetores de L, e os escalares v_{lk}, que são os M valores dos M autovetores de L e Φ_k, que são os M vetores da matriz C, sabe-se, a partir de (6) a (9), que:

$$AV = \sum_{k=1}^{M} v_{lk} \Phi_k, \ (l = 1,...,M) \tag{11}$$

Como (11) é verdadeira, ao invés de se usar a expressão (10) para calcular os autovetores de C, eles podem ser calculados de forma mais simplificada, a partir de combinação linear do espaço das imagens originais (matriz A) com os *autovetores* de L (matriz V), multiplicando-se as matrizes A e V, da seguinte forma:

$$U = AV \tag{12}$$

Onde a matriz V, de dimensão (MxM) é constituída pelos M *autovetores* de L e a matriz U, de dimensão $(N^2 xM)$ é constituída por todos os *autovetores* de C, e a matriz A naturalmente é o espaço de imagens, de dimensão $(N^2 xM)$.

Todos os *autovetores* têm um *autovalor* associado a si próprios e os *autovetores* com os maiores *autovalores* provêem mais informação sobre a variação da face do que os com *autovalores* menores.

Depois que as *eigenfaces* são extraídas da matriz de covariância de um conjunto de faces, a próxima etapa é o treinamento do modelo. Para isso foram usadas apenas 4 imagens de cada classe. Estas imagens, então, são utilizadas no treinamento do modelo. E para a verificação e testes do modelo são utilizadas todas as *M* imagens do conjunto de treinamento.

Todas as imagens representantes das classes são projetadas no espaço de *eigenface* e representadas por uma combinação linear das *eigenfaces*, tendo um novo descritor que corresponde a um ponto dentro de um grande espaço dimensional. Sabe-se que apenas alguns poucos *autovetores* com os *autovalores* maiores são suficientes para o reconhecimento facial, por isso foram usados apenas *(M´<M) autovetores*. Esta projeção se dá da seguinte forma:

$$\Omega_i = U^T (\Gamma_i - \Psi), i = 1,..., Nc. \tag{13}$$

Onde a matriz Ω_i, de dimensão $(M´xNc)$, contém os *Nc autovetores*, de dimensão $(M´x1)$, da matriz L, e é usada para comparação com as novas faces apresentadas para efeito de comparação e reconhecimento. O valor *Nc* é o número de classes existentes no conjunto de treinamento.

Se todos as *eigenfaces* forem usados para representarem as faces, esses conjuntos de imagens iniciais podem ser completamente reconstruídos. As *eigenfaces* são usadas para representarem ou codificarem qualquer face a ser comparada ou reconhecida. Deve-se usar *eigenfaces* com *autovalores* mais altos para reconstruir as faces porque eles provêem muito mais informação sobre a variação de faces.

Em função da projeção sobre o espaço de *eigenface*s descrever a variação de distribuição de faces, é possível usar estes novos descritores de faces para classificá-las. O Reconhecimento Facial se dá extraindo-se os descritores da nova face submetida a reconhecimento e comparando-os com os descritores das classes previamente armazenadas no banco de dados, calculados da mesma maneira. A metodologia utilizada para fazer esta comparação foi a distância euclidiana. Assim, cada face submetida ao Reconhecimento Facial é projetada no espaço de faces, obtendo-se o vetor Ω, da seguinte forma:

$$\Omega = U^T (\Gamma - \Psi) \tag{14}$$

O vetor Ω, de dimensão (*Mx1*), é comparado com cada um dos vetores Ω_i $(i = 1,...,Nc)$. Se a distância encontrada entre Ω e qualquer Ω_i $(i = 1,...,Nc)$ estiver dentro do *threshold* da classe e for a menor distância encontrada, então houve o reconhecimento facial de Ω pertencendo à classe *i*.

A distância é calculada por meio do método dos mínimos quadrados, da seguinte forma:

$$\varepsilon_i^2 = \|\Omega - \Omega_i\|^2, \ (i = 1,...,Nc) \tag{15}$$

Os *thresholds* θ_i $(i = 1,...,Nc)$ definem a distância máxima permitida entre a face nova submetida ao reconhecimento e cada uma das classes. Se a distância encontrada entre a nova face e uma das classes estiver dentro do *threshold* da classe, então houve o reconhecimento facial. Os *thresholds* são ajustados por uma variável *k*, que define o grau de tolerância a erros, quanto menor for esta variável, maior é a tolerância a "falsos positivos" e menor é a tolerância a "falsos negativos".

O cálculo dos *Nc thresholds*, em que *Nc* é a quantidade de classes trabalhadas, é feito da seguinte forma:

$$\theta_{ik} = \frac{1}{k} \max\{\|\Omega_i - \Omega_j\|\} \ (i, j = 1,...,Nc; \ k = 1,...,10) \tag{16}$$

Os *autovetores* das imagens de faces são definidos no espaço de imagem, eles podem ser vistos como faces e realmente são parecidos com faces, por isso eles são chamados de *eigenfaces*. A maior variação dos vetores de treinamento é descrito pela primeira *eigenface*. A segunda maior variação dos vetores de treinamento é descrito pela segunda *eigenface*, e assim por diante.

Cada *eigenface* pode ser vista como uma característica, quando uma face particular é projetada sobre o espaço de face, seu vetor (composto por seus valores de peso com relação a cada *eigenface*) no espaço de face mostra a importância que cada uma dessas características descreve na face.

Considerando-se que a imagem montada no espaço de faces é realmente uma face, o peso do primeiro *eigenface* é muito alto. O valor dos pesos diminui de acordo com o número dos aumentos de *eigenface*, o que está em conformidade com a definição de *eigenfaces*. O primeiro *eigenface* responde pela variação máxima, o segundo responde pela segunda variação máxima, e assim sucessivamente.

Ao contrário da detecção facial, em que há apenas duas classes de objetos, faces e não-faces, aqui cada indivíduo está numa classe separada. Todas as faces têm as mesmas características faciais e são basicamente bem parecidas na configuração global. Isto faz do reconhecimento facial um problema muito difícil e interessante. Outra coisa que o torna mais complicado é que a face de cada indivíduo pode ter muitas variações por causa da mudança de orientação, expressão facial, iluminação na imagem, escala e disfarces.

Uma imagem de face é um *array* bidimensional de valores de intensidade. Neste modelo apresentado o tamanho padrão proposto é de 128x128 pixels. Também pode ser tratado como um vetor ou um ponto em um espaço de dimensão 16384. Mas as imagens de faces não são distribuídas fortuitamente neste espaço dimensional alto. O fato de todas as faces serem basicamente bem parecidas umas com as outras e terem as mesmas características faciais, como olhos, nariz e boca, faz de todas as faces um subconjunto do espaço de imagem completo, em outras palavras, a dimensão do espaço de faces é menor do que o espaço da imagem.

7. RECONHECIMENTO FACIAL COM SEMI-OCLUSÃO DE FACES

Em aplicações forense, em que muitas vezes o criminoso é filmado na cena de crime com a face semi-oclusa, com máscaras ou outro artefato cobrindo parte do rosto, é necessário que o software possibilite o reconhecimento facial a partir apenas a região descoberta da face. Normalmente a parte descoberta é a região dos olhos, ou da boca ou do nariz [07, 08, 09, 10 e 11].

Assim, com o objetivo de viabilizar o reconhecimento facial automático com imagens semi-oclusas, os conceitos de *eigenfaces* estão sendo expandidos para *eigeneyes, eigenmouth* e *eigennose*, visto que o algoritmo desenvolvido unicamente baseado em *eigenfaces* responde muito mal quando as imagens estão semi-oclusas ou com problemas de iluminação. Esta técnica aqui apresentada pode ser bastante útil nas aplicações policiais, em que há a necessidade de reconhecimento de pessoas com

disfarces diversos, cobrindo parte do rosto, o que normalmente ocorre nas cenas de crimes, em que o criminoso se disfarça com máscaras cobrindo parte da face. Assim, com a utilização das técnicas desenvolvidas e aqui apresentadas, o reconhecimento facial automático se torna possível com a utilização de apenas partes pequenas da face. Utilizando-se as *eigenmouth* e *eigennose*, é possível o reconhecimento facial automático de pessoas com a parte superior da face coberta, com óculos escuros ou máscaras. Com a utilização da técnica de *eigeneyes* é possível é possível o reconhecimento de pessoas com a parte inferior da face coberta com uso de máscara, desde que com a região dos olhos exposta.

Os algoritmos desenvolvidos para esta técnica de *eigenmouth* e *eigennose* são muito semelhantes aos algoritmos de *eigenface*, tendo, no entanto, uma "inteligência" adicional para verificar automaticamente a parte da face que deve ser submetida a reconhecimento. Também terá que manter um banco de dados bem mais completo, com informações específicas de *eigenfaces, eigenmouth, eigennose* e *eigeneyes*, referentes a todas as classes trabalhadas, utilizando-se sempre os mesmos critérios estabelecidos na extração e confrontos de todas estas *eigenfeatures*.

Pode-se observar tanto visualmente, a partir da Figura 02, como com base nas planilhas com os resultados obtidos, a partir do processamento dos algoritmos de *eigenfeatures*, que estes algoritmos têm comportamento diferenciado em relação aos das *eigenfaces*.

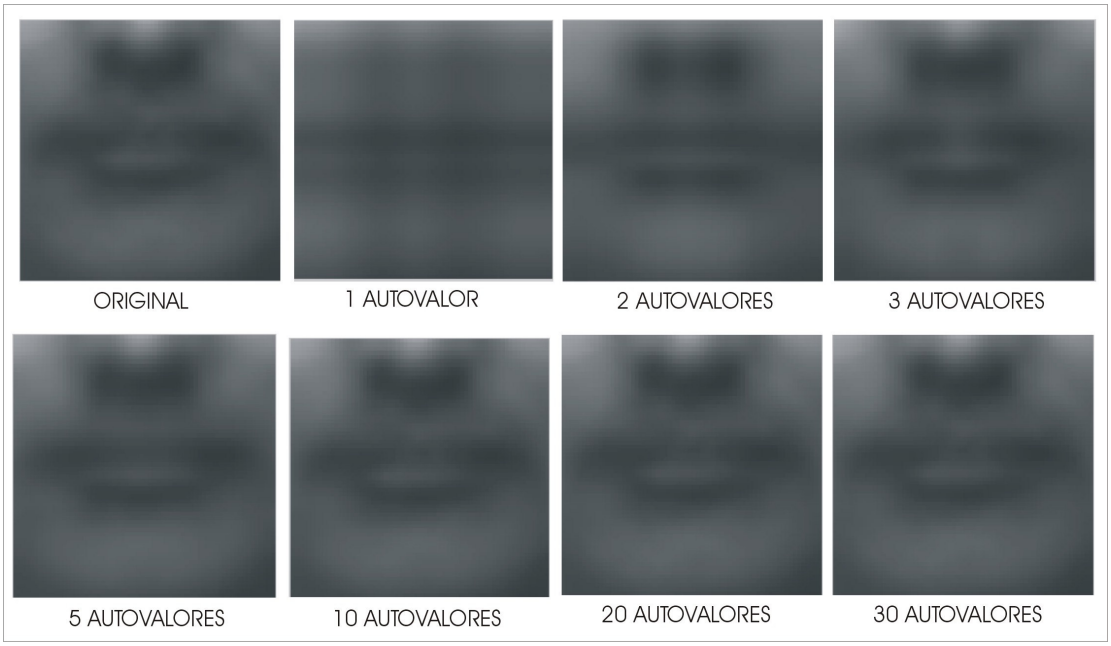


Figura 02. "Boca Média" original e várias reconstruções com os autovetores com os maiores autovalores.

O desempenho das *eigenfaces* é mais comportado, melhorando linearmente à medida que se aumenta o número de autovetores utilizados no reconhecimento, enquanto que o desempenho das *eigenfeatures* é um pouco inesperado, oscilando ligeiramente para cima e para baixo ao ser submetido a uma variação sempre crescente de quantidade de autovetores utilizados, conforme pode ser observado nas Tabelas 01, 02, 03 e 04.

Ainda com o objetivo de viabilizar o reconhecimento facial automático com imagens semi-oclusas, também é feita a expansão dos conceitos de *eigenfaces* para *eigeneyes*. Desta forma, dispondo-se de apenas uma região com aproximadamente 20% da face, pode-se fazer o reconhecimento facial. Foram desenvolvidas duas técnicas baseadas em *eigeneyes*: com o uso de apenas um dos olhos ou centrando os dois olhos. A primeira técnica apresentou melhores resultados, com melhores eficácias.

A Figura 03 ilustra a utilização da segunda técnica, em que os dois olhos são utilizados, e a Figura 04 foi produzida a partir da utilização da primeira técnica, em que se faz uso de apenas um dos olhos, e mostra algumas imagens dos olhos direitos das pessoas (esquerdo da imagem) utilizadas

nestes experimentos, em que é mostrado que o reconhecimento facial automático pode ser levado a efeito com apenas uma pequena parte da imagem da face. Na Figura 04, A é o "Olho Médio" de todo o conjunto de treinamento. B-D são os "Olhos Médios" de suas respectivas classes. E-H são alguns exemplos de imagens do conjunto de treinamento.

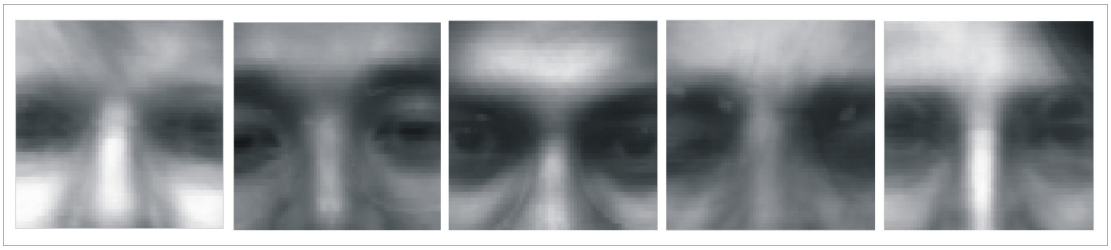


Figura 03. Técnica de *eigeneyes* com a utilização dos dois olhos.

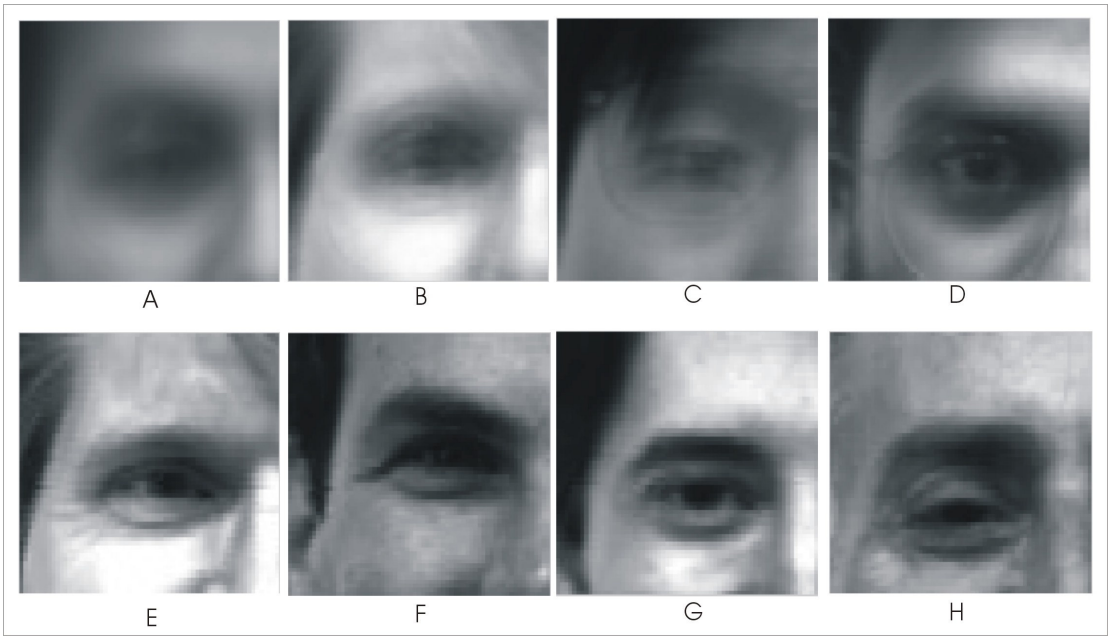


Figura 04. Técnica de eigeneyes com a utilização de apenas um olho.

8. RESULTADOS

A seguir serão mostrados os desempenhos apresentados pelo modelo em todas as situações em foi utilizado. A Tabela 01 apresenta os resultados com a utilização do algoritmo *eigenfaces*, com a utilização as faces completas das pessoas. Esses resultados são os melhores obtidos, com até 98,33% de acertos, com a utilização de 50 autovalores.

A Tabela 02 mostra os resultados obtidos com o algoritmo *eigeneyes*, com a utilização de um único olho conforme mostrado na Figura 04. Apesar da utilização de apenas cerca de 20% da face, os resultados obtidos por este algoritmo ficaram apenas 10,83% inferiores ao desempenho do algoritmo *eigenface*.

A Tabela 03 mostra os resultados obtidos com o algoritmo eigenmouth, conforme imagens mostradas na Figura 02, e a Tabela 04 apresenta os resultados do algoritmo eigeneyes, com a utilização da região em torno dos dois olhos, conforme imagens mostradas na Figura 03. Os resultados desses dois algoritmos ficaram ligeiramente inferiores aos resultados do algoritmo *eigeneyes* com um único olho.

AUTO VALORES	ERROS		ACERTOS	
	QTD	TAXA	QTD	TAXA
05	28	23,33%	92	76,67%
10	14	11,67%	106	88,33%
20	8	6,67%	112	93,33%
30	4	3,33%	116	96,67%
50	2	1,67%	118	98,33%

Tabela 01. Resultados do algoritmo *Eigenfaces*.

AUTO VALORES	ERROS		ACERTOS	
	QTD	TAXA	QTD	TAXA
05	32	26,67%	88	73,33%
10	19	15,83%	101	84,17%
20	20	16,67%	100	83,33%
30	19	15,83%	101	84,17%
50	15	12,50%	105	87,50%

Tabela 02. Resultados do algoritmo *Eigeneyes*.

AUTO VALORES	ERROS		ACERTOS	
	QTD	TAXA	QTD	TAXA
05	21	17,50%	99	82,50%
10	16	13,33%	104	86,67%
20	17	14,16%	103	85,83%
30	16	13,33%	104	86,67%
50	18	15,00%	102	85,00%

Tabela 03. Resultados do algoritmo Eigenmouth.

AUTO VALORES	ERROS		ACERTOS	
	QTD	TAXA	QTD	TAXA
05	38	31,66%	82	68,33%
10	31	25,83%	89	74,17%
20	26	21,66%	94	78,33%
30	25	20,83%	95	79,17%
50	23	19,16%	97	80,83%

Tabela 04. Eigeneyes do algoritmo com a região dos olhos.

9. APLICAÇÕES DO ALGORITMO EIGENFACE EM CASO REAL

O reconhecimento facial pode ser utilizado em muitas aplicações forenses, inclusive em perícia criminal, para efeito de reconhecimento de criminosos filmados ou fotografados em cenas de crime, como um caso real em que fizemos exame pericial com a utilização desse algoritmo *eigenface*, para o reconhecimento de dois assaltantes de bancos filmados na cena do crime.

Nesse caso, foram apresentados para exames periciais alguns filmes em arquivos com extensão avi, contendo filmagem de cena de crime, em que dois indivíduos praticavam assalto a uma agência bancária. Também foram apresentadas fotos de dois suspeitos que haviam sido presos. Foi solicitada a elaboração de exames periciais com o objetivo de responder se os dois suspeitos presos são os mesmos indivíduos filmados praticando o assalto à agência bancária.

Alguns problemas encontrados dificultaram os exames periciais. A resolução das imagens extraídas dos filmes da cena do crime era muito baixa, em que as faces recortadas das imagens têm menos do que 30x30 pixels. Além disso, como as câmaras foram colocadas em locais inadequados, os atores não aparecem de forma frontal e ereta, mas sim de perfil e de cabeça baixa. Na única foto em que um dos atores apareceu de forma frontal e ereta, o lado esquerdo do indivíduo veio cortado, em decorrência do posicionamento da câmara. Outro problema observado foi com relação às fotos questionadas, pois as mesmas não eram contemporâneas, sendo que uma delas foi tirada possivelmente há mais de dez anos antes do crime.

Com relação ao material questionado, as fotos apresentadas inicialmente foram desconsideradas, tendo sido tiradas novas fotos dos suspeitos presos, para efeito de utilização das mesmas como padrão. Procurou-se tirar fotos nas mesmas posições em que se apresentaram os atores nas cenas do crime, para facilitar as comparações. Quanto às imagens obtidas dos filmes de baixa resolução, foram selecionadas as melhores fotos nas melhores posições. A foto em que um dos atores teve o lado esquerdo cortado foi reconstruída, por meio de técnicas de processamento de imagens, partindo-se da premissa de que os dois da face das pessoas são simétricos, obtendo-se, a partir desta foto, os melhores resultados.

10. CONCLUSÕES

O modelo proposto é bastante robusto no tratamento de imagens de faces obtidas em condições controladas de iluminação, inclusive com expressões faciais variadas e uso de óculos transparentes.

Ele é bastante eficiente e simples tanto na etapa de treinamento como na de reconhecimento, dispensando a necessidade de processamentos de baixo nível para verificações da geometria da face ou das distâncias entre os órgãos faciais e/ou de suas dimensões.

Para efeito de dar um tratamento mais eficaz nas imagens com faces semi-oclusas ou incompletas, com disfarces, com máscaras ou óculos escuros, os conceitos de *eigenfaces* foram expandidos para *eigeneyes*, *eigennose* e *eigenmouth*, procurando-se o reconhecimento facial a partir de fragmentos da imagem de aproximadamente 20% da face, viabilizando-se o reconhecimento facial a partir de imagens semi-oclusas, incompletas, com disfarces, mal-iluminadas ou apresentadas em perfil.

O software pode ser utilizado em casos reais para o reconhecimento de pessoas em cenas ce crime, por meio da comparação das imagens encontradas nessas cenas com imagens das faces de suspeitos, em atendimento a solicitações específicas ou em comparações com bancos de dados de listas negras, compostas de criminosos e suspeitos em geral.

11. REFERÊNCIAS BIBLIOGRÁFICAS

[01] Bruce, V. e Young A., "In the Eye of the Beholder", Oxdford University Press, 280 pp., 1998

[02] Brunelli, R. e Poggio, T, "Face Recognition: Features versus Templates", IEEE Transactions on Pattern Analysis and Machine Intelligence 15(10), páginas 1042 a 1052, 1993.

[03] Cantor, N. and Mischel, W., "Prototypes in person perception.", In L. Berkowitz, editor, Advances in Experimental Social Psychology, volume 12, páginas 3 a 52, Academic Press, 1979.

[04] Hay, D.C. and Young, A.W., "The Human Face", In A.W. Ellis, editor, Normality and pathology in cognitive functions, páginas 173 a 202. Academic Press, 1982.

[05] Manjunath, B. S.; Chellappa, R. e von der Malsburg, C., "A Feature Based Approach to Face Recognition", Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Champaign, Illinois, USA, 1992.

[06] Proesmans, Marc e Gool, Luc Van, "Getting Facial Features and Gestures in 3D", Katholieke Universiteit Leuven, Face Recognition From Theory to Applications, NATO ASI Series, Series F: Computer and Systems Sciences, Vol. 163, Springer-Verlag Berlin Heidelbert, 1998.

[07] Quintiliano, Paulo e Santa-Rosa A., "Face Recognition Based on Eigenfeature". **In:** Proceedings of SPIE Second International Symposium on Multispectral Image Processing and Pattern Recognition, Wuhan/China, pp. 140-145, 2001.

[08] Quintiliano, Paulo; Guadagnin R. e Santa-Rosa, Antônio, "Practical Procedures to Improve Face Recognition Based on Eigenfaces and Principal Component Analysis". Pattern Recognition and Image Analysis, Vol. 11, No. 2, pp. 372-376, The Russian Federation, 2001.

[09] Quintiliano, Paulo e Santa-Rosa, Antônio, "Face Recognition Based on Symmetryzation". **In:** Proceedings of the International Conference on Computer Science, Software Engineering, Information Technology, e-Business, and Applications (CSIT e A'02), CSITeA02, V. 1, pp. 109-114, 2002.

[10] Quintiliano, Paulo e Santa-Rosa, Antônio, 2003. "Face Recognition Based on Eigeneyes"., Pattern Recognition and Image Analysis, Vol. 13, No. 2, pp. 339-342, The Russian Federation, 2003.

[11] Quintiliano, Paulo e Santa-Rosa, Antônio, 2003, "Face Recognition Based on Eigeneyes and Eigenfaces". **In:** Proceedings do XIII Congresso Mundial de Criminologia, Rio de Janeiro, 2003.

[12] Sobottka, Karin e Pitas, Ioannis, "Localization of Facial Regions and Features". The 4-th Open Russian-Geerman Workshop Pattern Recognition and Image Analysis", Novgorod State University, The Russian Federation, March 3-9, 1996.

[13] Young, A. W., "Face and Mind", Oxford University Press, 405pp., 1998.

MANET AUTO CONFIGURATION WITH DISTRIBUTED CERTIFICATION AUTHORITY MODELS CONSIDERING ROUTING PROTOCOLS USE

Robson de Oliveira Albuquerque[1] , Maíra Hanashiro [1], Yamar Aires da Silva [2], Rafael Timóteo de Sousa Jr. [3], Paulo Roberto de Lira Gondim[1]

Universidade de Brasília
Campus Universitário Darcy Ribeiro
Faculdade de Tecnologia
Depto de Engenharia Elétrica e Redes de Comunicação
Laboratório de Redes - sala B1
CEP: 70910-900 - Brasília - DF – Brazil
[1]{robson, maira,pgond}@redes.unb.br
[2]{yamar.silva}@siemens.com
[3]{desousa}@unb.br

Abstract

In this paper, we discuss about certification, authentication, auto configuration and routing for mobile ad hoc networks (MANETs). The presented design is based on the works [1], [2] and [3]. We describe distributed certification, MAE authentication, auto configuration process and routing protocols. Then, we show some problems of these models and we propose some solutions considering routing and others protocol modifications.

Key words: *MANET, certification, authentication, routing protocols, auto configuration.*

1. INTRODUCTION

Wireless networks are defined as computers networks that are connected to its work area through wireless links, such as radios frequencies and infrared rays. Wireless local area networks (WLAN) arised with the main purpose to overcome the limitations imposed by traditional wired networks, thus permitting faster network installations and mobility.

According to 802.11 [4] standard, established by the IEEE board founded in 1990, WLAN can be sorted in independent networks (Ad Hoc) and access point dependent.

In an infrastructured WLAN (based in access point) all communication among mobile nodes (MN) goes through mobile support stations (MSS) and usually it is directly connected to a wired network. In this situation MN cannot communicate among each other directly.

In Ad Hoc WLAN, refered as Mobile Ad Hoc NETwork (MANET) by IETF, MN can communicate with each other because there is no MSS. In this kind of networks, MN does not require any physical infrastructure and nodes can move freely because there is no central communication point.

Ad Hoc WLAN are mostly used in situations where it cannot or does not make any sense, install a fixed wired network, such as disaster situations, hurricanes, earthquakes, where rescue teams needs coordination and communication. Soldiers in a battlefield exchanging tactical information, businessman receiving information in business meetings, students using laptops in classrooms. In a near future, Ad Hoc networks shall have an important paper in wearable computers interconnection, sort of future computer that can be attached to human body, for example, a computer jacket.

An Ad Hoc WLAN can operate isolated or it can be an extension of some wired network already installed, which, in this case, needs a communication gateway to connect each other.

As advantages of MANET it has quickly installation (can be installed in areas with no previous infrastructure because it needs no fixed base to route messages), fault tolerant (any malfunction or disconnection of a station can be easily solved with dynamic reconfiguring of the network),

connectivity (if two stations are inside the same area where there is reach of radio waves, there is a communication channel), mobility and others.

Based in RFC 2501 [5], some characteristics and fragilities are important in these networks. These characteristics and fragilities are related to dynamic topologies, restricted bandwidth and variable links capacity, power save consumption operation and limited physical security.

Due to these problems, MANET needs proper specifications related to certification, authentication, configuration and routing.

In this paper some proposals related to certification and auto configuration with routing considerations are presented and fundamented in [1] and [2] developed work. Besides that, some problems are emphasized and possible solutions are shown as considerations and possible solutions related to auto configuration and distributed Certification Authority (CA).

2. MANET ROUTING PROTOCOLS

Routing protocols are responsible for finding, establishing and keeping routes between MN that wishes to communicate. It is very important that routing protocols in MANET creates very few messages as possible, avoiding network overhead and thus not consuming network bandwidth. These factors are directly connected with the velocity that network routes are established and the frequency that they are updated. Different techniques were developed creating protocols that can create and establish routes faster than others. Others can consume less bandwidth but takes more time to establish a specific route.

According to IETF MANET workgroup [4], there is a desirable quality list that routing protocols are required to supply with: (a) distributed operation, (b) no routing loops, (c) under demand operations, (d) pro-active operation, (e) security, (f) inactivity period operation and (g) unidirectional link support.

Basically MANET routing protocols can be classified as reactive and pro-active. Pro-active are routing protocols that keep information about routes to every MN in the network. Reactive protocols only create a route when it is requested by origin node.

Four routing protocols are specified by IETF with drafts RFC: (a) TBRPF [6], (b) OLSR [7], (c) AODV [8] and (d) DSR [9]. Where (a) and (b) are considered pro-active routing protocols and (c) and (d) are considered as reactive routing protocols.

Topology Dissemination Based on Reverse-Path Forwarding (TBRPF) creates per hop routing by the shortest path for each destination. Each MN running TBRPF generates a topology information tree based in information topology that is saved in a topology table. To minimize network processing, each MN reports only a few portion of is topology table to neighbor MN. TBRFP uses different combinations and periodical updates to keep every MN informed about its own topology tree. To reach and keep robustness in highly mobile environments in the protocol, each MN can send additional information (complete topology tree) to its neighbors.

Differentiated HELLO messages are used to neighbor discovery that contains only information about neighbor change. This modified message results in shorter messages based in link state algorithm.

TBRPF can be divided into two main modules. The first module is called "neighbor discovery" and the second is called "routing" which does the topology discovery and computes the routes to every destination.

Optimized Link State Routing Protocol (OLSR) has as key concept the use of multipoint relays (MPRs). MPRs are MN selected to forward broadcast messages in the routing protocol flooding mechanism. MPRs are spread throughout MANET to provide every MN the partial information about the necessary topology that computes the best route to every MN in the network. MPRs combined with local duplicity avoidance are used to minimize the number of control packets that should be sent in the network.

OLSR is projected to work in high scalable networks where traffic is sporadic and randomly among specifics MN. As a pro-active protocol, it is also adequate to scenarios where pairs of MN changes very often, but no additional control packet is generated in the network since the routes are kept and known by all possible destination.

Ad hoc On-Demand Distance Vector Routing (AODV) is based in Destination-Sequenced Distance Vector Routing Algorithm (DSDV) protocol. In general AOADV tries to cut off the need of broadcast routing messages, which limits its own scalability. Another important AODV point is that it tries to minimize the latency when new routes are required.

AODV is classified as distance-vector algorithm and is considered as a reactive protocol because only one route is created if it is necessary. In general, AODV tries to eliminate the broadcast routing messages flooding, which limits its own scalability. AODV also tries to minimize latency when new routes are requested. It functions is similar to traditional algorithms what can facilitate the interconnection with wired networks. Even though working very closed to traditional protocols, AODV allows multicast and unicast traffic, however the protocol shows only one route to every destination what cannot be a good characteristic.

Dynamic Source Routing (DSR) is a simple and efficient routing protocol designed to multi-hop MANET with up to 200 MN and supports high mobility rates. It allows the network to organize and auto configure itself without the network infrastructure administration.

DSR is divided into two main modules: "routing discovery" and "routing maintenance" that work together to permit that MN discover and keep updated routes. All aspects of the protocol work under demand, thus not sending periodical messages to routing exchange information. This characteristic of the protocol allows low network bandwidth consumption and power saving.

DSR also permit multiple routes to a specific destination and that every sender selects and control the used routes to forward its packets. Other advantage of the protocol is that is provides loop-free routing information, supports unidirectional links and fast convergence when the network topology changes.

3. MANET ROUTING PROTOCOLS

To avoid malfunction in MANET it is necessary security in message routing. Besides in [3], [10] and [11] an authentication service for routing protocols is proposed, where Manet Authentication Extension (MAE) is used and attached to every message in the routing protocol. All necessary information to authentication are included in MAE. The main focus of the proposed model was to keep the routing packets and its messages unchanged. MAE format is shown in Fig.1.

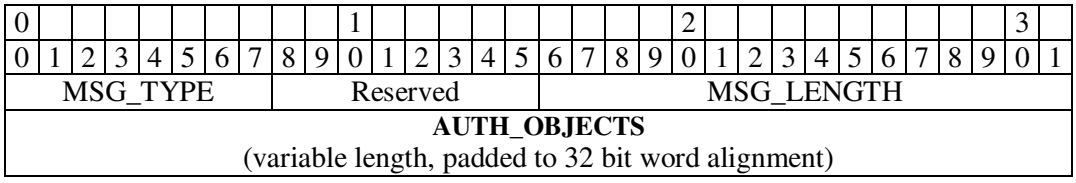


Fig. 1 – MAE Syntax

MSG_TYPE field is used to differentiate MAE messages from other routing protocol messages. MSG_LENGTH field indicates the size of MAE in bytes and AUTH_OBJECTS has the objects that have authentication information.

4. DISTRIBUTED CERTIFICATION

In MANET, due to its characteristics, is heavily not recommended any centralized service. In [12], [13] and [1] approach a distributed certification model is proposed.

The model proposed uses threshold cryptography theory and pro-active secret key update based in Shamir [14] schema.

In the system point of view, the whole architecture is fully distributed and the service is localized using a coalition approach and the cryptographic system is fully based in RSA model.

It is considered a MANET where every NM v_i has a personal RSA key pair $\{sk_i, pk_i\}$, where $sk_i =< d_i, n_i >$ is the private key and $pk_i =< e_i, n_i >$ is the public key that are used in point-to-point transactions.

A Certification Authority (CA) has a key pair $\{SK, PK\}$, where $SK =< d, n >$ is used to sign all MN certificates. Any certificate in this approach can be verified by the system public key SK, that is know by ever MN in the network.

According to threshold cryptography, SK is divided in the network. Every MN v_i, besides its own key pair, has the partial key P_{vi}. Any subgroup k of n MN can work as a CA. However it is not possible to any MN to know SK, but in the system initialization.

Threshold cryptography is indicated in MANET due to some of its proprieties: (a) the distribution and decentralized control of the keys fits the profile of Ad Hoc networks, (b) security omnipresence is guaranteed since the secret is fully distributed in the network and intrusion detection is more practical and efficient, (c) the limit k is the balance between the service availability and intrusion tolerance. In other words, a group of adversaries need to destroy $(n-k+1)$ partial key holders to bring the system down (once it would block one auto configuration) and at least break k partial keys to steal SK secret.

System is initialization is a very careful step to k choosing. As lower the k value the greater the facility of break SK secret. In other hand the greater the value of k the higher the system security, which reduces fault tolerance at the same time. After all, the most close k is from n, the probability of $(n-k+1)$ MN leaving the network raises, which would forbid the service.

Certificates generated by a CA formed by a subgroup of k MN have the finality of certificate, as in a normal cryptographic system, the public key of every MN. Therefore, every MN has its own $cert_i$ certificate that must be signed by SK, in $< v_i, pk_i, T_{sign}, T_{expire} >$ format, where v_i is the MN identifier, pk_i is its public key, T_{sign} is the signature date and T_{expire} is the expiration certificate date.

To control the certificate validity are used to methods: (a) Implicit certificate revocation that defines that every MN must renew its certificate at least ever period T_{renew} where $T_{expire} \leq T_{sign} + T_{renew}$, (b) explicit certificate revocation where a certificate is assumed by Certificate Revocation List (CRL) is not valid anymore even its T_{expire} is valid. This implies directly that only revoked certificates that did not expire must be in CRL.

This model was implemented in [1] which involves only subgroups, k size, of partial key holders. The basic operations include: (a) secret key negotiation, where the secret key can be obtained by on MN with the system initialization or with the auto configuration service. In the first case, both keys and certificates are distributed to MN by a central negotiator before MANET formation. In the second case, an auto initialization algorithm where k MN can provide a partial key to new MN in the network, (b) the secret key update, instead of changing the system key from time to time, only changes the partial key with the main purpose of protecting the secret key from being broken. The system supports until $k-1$ partial secret breaks because SK is obtained with k keys. If in a update situation there is less than k discovered keys, SK is protected and does not need to be changed, (c) the certification service permits, that when a MN requests using the certification service, one subgroup of k (coalition) partial secret key holders is created and every MN v_i generates a partial signed certificate to the requesting MN. MN then generates its certificate by grouping k received certificates that represents a signed certificate from SK. This service includes emission, renovation and

revocation of certificates, besides, even before the MANET formation, a security policy for each step should be defined.

5. AUTO CONFIGURATION

A MN to communicate in a network must have a unique identifier, usually the IP address. However, in MANET the topology changes dynamically thus creating a difficult environment for centralized administration that can distribute IP address or any other identifier. This situation leads to a distributed, dynamically and automatic service.

Together with security and routing protocols, auto configuration provides a service that can became MANET more efficient and robust. Even though there are many approaches related to auto configuration, none has been standardized.

In [14] is proposed an auto configuration model that uses message authentication considering the distributed CA model in [12], [13] and [1]. In [2] approach a protocol for auto configuration is developed considering a distributed CA, which avoids that any intruder MN can produce messages or even change the messages already created with the purpose to break the protocol or get the service unavailable. To reach this situation in MANET, according to [2], the MN where already configured with a valid certificate before they can request and join the auto configuration service.

Therefore to a MN request an IP address or even respond to MN client solicitation, MN must have a valid certificate. The authentication service of the auto configuration mechanism is supplied by MAE, which has all the necessary information to guarantee authenticity, integrity, non-repudiation in all MAE protected messages.

MAE used for the proposed auto configuration model is the same proposed to protect the routing messages in MANET routing protocols.

As cited before MAE has authentication objects which includes Digital Signature (DS) that is mandatory and authenticate all non-mutable fields of auto configuration messages. MAE should have one more object, that can be the certificate. The message sender must use DS with its private key because the certificate that goes with MAE has the sender public key that can be used to certify the message sender. If the MN certificate is not locally available, MAE can have a CERT object, which carries with the message the certificate that created and signed MAE. Additional objects are used to provide additional services that are beyond the protocol auto configuration approach.

Every NM that is valid and trustable belonging to MANET has an IP address identifying its interfaces and a subset of free IP address (FIA) to offer to MN clients that wishes do associate to the network. Inside an individual MANET, A MN FIA must be distinguished from others MN FIA thus avoiding that the same IP address can be distributed by more than one MN, besides that, every MANET has a unique identifier defined as partition ID (PID), which, in this situation permits that to MN that has the same PID are in the same MANET. PID also helps distinguishing different MANET in a specific area and also helps different MANET to be brought together.

Dynamic Configuration Distribution Protocol (DCDP) is used to distribute network configuration information such as IP address, network mask and default gateway, which uses binary division to provide to MN different IP address in the network. Binary division assures that all MN receives distinguished IP address, thus avoiding IP address conflicts even in a MANET join situation.

IN [2] To obtain and associate an IP address the MN must have received its valid certificate. When a MN wishes to join a MANET so it can obtain an IP address, it sends an ADDR_REQ message in broadcast using its MAC address as source address. Any MN belonging to the MANET answers the message with ADDR_REP that contains FIA with the biggest free IP quantity because a MN can have more than one FIA with different quantities. The MN can receive more than one answer from different other MN and then selects the MN that has the biggest FIA sending a SERVER_POOL message directly to the chosen MN server, discarding all other received messages.

The SERVER_POOL message confirms the MN intention of getting an IP address. The elected MN server then divides its FIA, sending one half to the MN that requested it and keeping the other half so it can answer future requests. The MN that received the FIA throughout IP_ASSIGNED message assigns the free IP address in its own FIA. The first IP address the MN uses for itself associating it with its interface and using all the rest as FIA to answers MN client requests.

If a MN has more than on FIA, for security and implementation facility reasons, the MN must mark in which FIA is its own address. The process is finished using an IP_ASSIGNEMENT_OK message to the server MN.

6. RELATED PROBLEMS AND PROPOSED SOLUTIONS

In [1] a MANET distributed CA was created and implemented. The proposed model relies in k size. This implies directly that k MN must be reached so a MN can have its certificate signed. If k MN are not reached, the MN cannot join MANET because it cannot sign its certificate. A routing protocol should then be used to reach k MN thus permitting the certificate signature.

Another problem related to k is that it has a fixed value that is defined considering a relative size so that k cannot have a big value (close to the total amount of MN in the MANET) and neither very short size (related to the quantity of MN in MANET). However the size of MANET is highly variable thus implying that an adequate defined k value may become inadequate considering that a MN can leave or join the MANET at anytime.

An initial solution is that k may vary in function of the size of the percentage of the network, but alter k is important define maximum and minimum values (both related to a percentage of the size of the network) of MN in function of the security necessity of the network and these values should be monitored as the quantity of MN in the MANET raise or reduce, thus implying directly that if a minimum or a maximum value is overpast is necessary a redefinition of k. According to the analyses of the results obtained in [1], the value of k can be defined as an average of the maximum and the minimum size.

Considering that k may vary from time to time, the model needs improvements in the CRL because the number of revoked certificates would be much bigger because the certificates are fully dependent on k. At this point we have the relation that the most k varies the most will be the emission of revoked certificates and the most will be the emission and requests of new certificates. This generates more traffic in the network and thus forcing the MN to process new certificates raising power consumption. Besides the variation of k, as MN enter and leaves the network, the certificates are automatically revoked but new certificates needs a new CA initialization. But according to [1] the process of CA initialization is centralized, contradicting the MANET's necessity.

In [1] model approach, to solve out this problem here presented is necessary the creation of a model of distributed CA initialization that implies in new mathematical models to the generation of a distributed key.

In other hand if k MN has to be reached, these MN can be reached using routing protocols to the signature of a previous requested certificate. This problems requires that a MN can work as a proxy, asking in the MN's name that others $k-1$ MN sign the certificate request. Considering that the proxy MN already has a valid configuration in the network related to IP address it could request the certificate to be signed using routing measures if $k-1$ could not be reached for itself.

Another approach considers that it could be used a temporary IP address to request the certificate signature. This implies that a topology change is required because of the temporary IP chosen by the MN. To solve out this problem a range of IP network address (even in CIDR) could be allocated and announced in the network informing that if a MN wishes to sign a certificate so it can join MANET, it then should use an IP address range reserved to that finality.

Considering this situation OLSR could be used as routing protocols because of its pro-active characteristic, besides the information messages to the reserved IP range could be announced by MPRs. A time-to-live (TTL) should be limited to 2 or 3 hops because is highly probable that $k-1$ nodes could be reached by routing. Another consideration is that it would limit the traffic related to certification signatures.

Another point is that any pro-active routing protocol could be used in this situation because the routing information would be easily created because the IP range would be well-known in the network.

In [2] the distributed CA approach implemented in [1] was used and the routing considerations where not applied limiting the reach of the auto configuration model proposed. This returns to the considered approach pointed herein because in [2] is assumed that the MN already has a valid signed certificate. So the proposed solution to [1] can be easily applied in [2].

Another problem in [2] is that the auto configuration model relies in that every message sent in the network is broadcast messages. This process makes the proposed auto configuration model not scalable because in huge MANET the amount of messages would increase significantly creating problems related to unnecessary bandwidth consumption and increasing power consumption by the MN.

To solve out this specific problem the protocol should be changed so that only the first message is broadcasted to reach all close MN. In this message the MAC address of the MN goes with the frame. As the MN server receives the sender MAC address the other messages in the communication process can be done in the unicast approach thus avoiding the flooding of the network.

7. CONCLUSIONS

MANET is increasing highly but some problems should be fixed out due to its characteristics. Related problems about auto configuration, routing measures, distributed CA are increasing as MANET standards are developed.

The approach studied in this paper is related to the problems found in [1] and [2] and the proposed solutions considering routing and others protocol modifications so both models can be more heavily developed and studied.

In [1] approach the proposed solution relies in static k, but in MANET the number o MN cannot be easily predicted. In other hand k is defined considering n. As n increases or reduces, k cannot vary because the whole process needs an initialization to secret key creation that is centralized. This approach was not considered in the implemented model and thus pointed herein to future researches in this subject. The initial proposed solution is based in new idea that relies in a fully distributed CA initialization approach so k can vary according to the necessity of MANET. It is important to say that this model should be heavily studied to validate the proposed solution.

In [1] the routing measures to reach k is not considered because it assumes that k are close of the requesting MN, which in MANET may not be true due to its mobility. An initial proposed solution considers that routing protocols can be used as proxy to reach k MN in order to produce a signed certificate.

In [2] the model is based in broadcasts messages during the whole auto configuration process. This paper proposes that the protocol should be changed in order to avoid unnecessary bandwidth consumption and thus avoiding power consumption. Once the first message is sent the MAC address of the sender can be easily obtained and the consequent communication process can be done using unicast approach.

Both [1] and [2] are heavily fundamented and very well work were developed permitting that new approaches and researches could be conducted using both proposed models in order to allow secure auto configuration and distributed CA in MANET.

8. REFERENCES

1. SILVEIRA, F. AND HANASHIRO, M., Serviços de Certificação para Redes Móveis Ad Hoc. UnB, Brazil, 2003.
2. BUIATI, F.M., Protocolo Seguro para Autoconfiguração de Endereços de Redes Móveis Ad Hoc, UnB, Brazil, 2004.
3. PUTTINI, R.S., ME, L., e SOUZA, R. T. de, Certification and Authentication for Securing MANET Routing Protocols.
4. IEEE Standard 802.11, Wireless LAN media access control (MAC) and physical layer (PHY) specifications, First edition, 1999-08-20
5. CORSON, S. e MARKER, J., Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation consideration. RFC 2501 (informational), IETF, 1999.

6. OGIER, R., LEWIS, M., TEMPLIN, F. e BELLUR, B., Topology Dissemination Based on Reverse-Path Forwarding (TBRPF), INTERNET DRAFT, MANET working group, <draft-ietf-manet-tbrpf-06.txt>, November 2002.
7. CLAUSEN, T. e JACQUET, P. Optimized Link State Routing Protocol, IETF Internet Draft, MANET working group, version 11, Jul. 2003.
8. PERKINS,C. E., ROYER, E. M. e DAS, S. R.. Ad hoc on-demand distance vector (AODV) routing. IETF INTERNET DRAFT, MANET working group, Jan. 2002. draftietfmanetaodv10.txt.
9. JOHNSON, D. B. et al, The dynamic source routing protocol for mobile ad hoc networks (DSR), INTERNET DRAFT, MANET working group, < draft-ietf-manet-dsr-07.txt>, Feb. 2002.
10. PUTTINI, R.S., ME, L., e SOUZA, R. T. de, An Authentication Protocol to MANET.
11. BUIATI, F.M., PUTTINI, R.S. e SOUZA, R.T.J. de, Secure Autoconfiguration for Móbile Ad Hoc, 2nd International Information and telecommunication Technologies Symposium I2TS 2003.
12. LUO, H. AND LU, S. Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks. Technical Report TR-200030, Dept. of Computer Science, UCLA, 2000.
13. KONG, J., ZERFOS, P., LUO, H., LU, S. AND ZHANG, L., Providing robust and ubiquitous security support for MANET, IEEE ICNP 2001, 2001.
14. SHAMIR, A. How to Share a Secret. Communications of the ACM, 22(11):612-613, 1979.

DETECÇÃO DE ATAQUES COM BASE NA VIOLAÇÃO DOS PROTOCOLOS IP E TCP

Norma Rodrigues Gomes[1], Luiz Antonio da Frota Mattos[2]

[1]Instituto Nacional de Criminalística – Departamento de Polícia Federal (DPF)
Setor Policial Sul – 70.610-200 – Brasília – DF – Brazil
[2]Departamento de Ciência da Computação – Universidade de Brasília (UnB)
Campus Universitário Darcy Ribeiro – 70.910-900 – Brasília – DF – Brazil

norma.nrg@dpf.gov.br, frota@unb.br

Abstract

One of the big challenges in network intrusion detection´s area is the limitation imposed by the use of well-known attacks signatures, disabling the previous detection of new attacks. This work presents a packet analysis methodology whose purpose is to detect anomalous behaviors, not basing on attacks signatures but verifying if the network protocols are not being violated, basing on the content of the respective headers. The biggest benefit is the possibility of anomalies or inadequate behaviors detection, that can correspond, total or partially, to variations of well-known attacks and even unknown.

1. INTRODUÇÃO

Com o uso das redes de computadores, juntamente com um grande avanço tecnológico, vieram também problemas relacionados a questões de segurança. Um mecanismo de segurança que vem ganhando cada vez mais espaço é o SDI - Sistema de Detecção de Intrusão. A maioria dos SDIs baseia-se em assinaturas de ataques, as quais, basicamente, descrevem padrões de comportamento conhecidos, considerados suspeitos e que constituem problemas de segurança [Amoroso, 1999].

Entretanto, um dos grandes desafios na área de detecção de intrusão é a limitação imposta pelo uso de assinaturas de ataques conhecidos, incapacitando a detecção prévia de novos ataques com assinaturas desconhecidas [Krügel et al., 2002].

Nossa proposta consiste em realizar uma análise de pacotes cuja finalidade é detectar a existência de comportamentos anômalos, mas não com base em assinaturas de ataques e sim verificando se os protocolos de rede não estão sendo violados, com base no conteúdo dos respectivos cabeçalhos. Com esse tipo de análise, além de ser possível detectar alguns tipos de ataques conhecidos, incluindo até mesmo possíveis variações destes, novos ataques, que façam uso de alguma violação de protocolo ainda não utilizada em nenhum ataque conhecido, poderiam ser detectados.

Neste artigo será apresentada uma metodologia de análise de pacotes, visando detecção de ataques, baseada na especificação dos protocolos IP e TCP. A Seção 2 apresenta informações sobre o problema causado por pacotes que violam protocolos de rede. A Seção 3 mostra a consistência da análise de pacotes proposta, definindo os métodos empregados. A Seção 4 compara o método em violação de protocolos com o baseado em assinaturas de ataques. A Seção 5 resume as conclusões obtidas e apresenta caminhos futuros para aprimoramento do trabalho proposto.

2. DESCRIÇÃO DO PROBLEMA

Em uma rede de computadores, a interação entre os diversos hosts que a compõem ocorre através do uso de protocolos, cujas especificações devem ser seguidas. Entretanto, é possível montar pacotes que violem os protocolos de comunicação, causando reações inesperadas no lado receptor dos pacotes, podendo configurar, inclusive, uma forma de ataque.

Uma rede de computadores está vulnerável a sofrer diversos tipos de ataques com múltiplos propósitos, tais como: fazer reconhecimento da rede (scanning de rede) para identificar serviços ou o

sistema operacional utilizado, interromper ou negar acesso de usuários legítimos a serviços, servidores ou outros recursos (negação de serviço ou DoS – Denial of Service), dentre outros.

Mecanismos de segurança têm sido desenvolvidos para detectar ataques a redes de computadores, dentre os quais destaca-se o SDI (Sistema de Detecção de Intrusão). A grande maioria dos SDIs baseia-se em assinaturas de ataques. Na prática, acontece que, uma vez ocorrido o ataque, o seu comportamento é analisado e é gerada uma espécie de regra que traduz esse comportamento, de forma que, sempre que esse comportamento ocorrer o respectivo ataque é detectado.

Entretanto, os SDIs que contam com comparação de padrões que representam assinaturas de ataques conhecidos, são incapazes de detectar previamente ataques não vistos com assinaturas diferentes, o que representa um dos grandes desafios na área de detecção de intrusão. Uma abordagem que vale a pena ser trabalhada, de acordo com [Allen et al., 2000], é ter uma noção do que constitui comportamento de sistema normal e detectar divergências a partir deste. Tal abordagem para detectar ataques desconhecidos consiste em determinar o que representa comportamento normal dentro de redes, *hosts* ou aplicações, e sinalizar atividade que não reflete o que é esperado.

Ao observar as assinaturas de ataques, nota-se que algumas delas representam, na verdade, violações aos protocolos de rede (por exemplo, TCP/IP), que deveriam ser seguidos. Assim, é importante entender como é o comportamento padrão dos protocolos envolvidos no tráfego de dados de uma rede, a fim de detectar se o mesmo atende às especificações do protocolo em questão. Tais especificações são definidas em documentos denominados de RFC (Request For Comments), que descrevem padrões esperados para protocolos individuais [Northcutt et al., 2000].

Portanto, ao verificar o protocolo que está sendo utilizado em uma dada rede, bem como suas respectivas especificações, definidas em RFCs, alguns comportamentos anômalos podem ser detectados, tornando, inclusive, desnecessária a existência de algumas assinaturas de ataques e possibilitando a detecção de algumas variações de assinaturas existentes.

3. ANÁLISE DE PACOTES PARA DETECÇÃO DE VIOLAÇÃO DE PROTOCOLOS

Nossa proposta consiste em realizar uma análise de pacotes cuja finalidade é detectar a existência de um comportamento divergente daquele esperado e definido pelo protocolo que estiver sendo utilizado. Para tanto definimos o escopo de trabalho, em termos de protocolos e tipos de análise, métodos para formalizar as regras de comportamento esperado de um dado protocolo, e uma implementação desse analisador de pacotes, em nível de protótipo, conforme detalhado a seguir.

3.1. Escopo da Análise de Pacotes

Dada a popularidade dos protocolos TCP/IP, o escopo definido para realização da análise de pacotes compreende os cabeçalhos IP e TCP. Assim, como trabalharemos com TCP, que é um protocolo confiável orientado a conexão, a análise dos pacotes será feita em duas etapas, a saber:

- Etapa 1 – Análise sem Estado (Stateless Inspection)
- Etapa 2 – Análise com Estado (Stateful Inspection)

Na Análise sem Estado é feito o exame de pacotes individuais, ou seja, a análise fica restrita ao conteúdo dos campos dos cabeçalhos de um pacote em questão, sem se preocupar em manter uma trilha do estado da conexão TCP/IP.

Já na Análise com Estado é feito o exame de uma seqüência de pacotes, ou seja, a análise engloba dados de cabeçalhos de mais de um pacote, permitindo detectar padrões de comportamento entre seqüências de pacotes e realizar correlações. Este artigo enfatiza os métodos e os resultados relativos a esta Etapa 2 da análise de pacotes proposta.

3.2. Análise sem Estado

A primeira etapa da análise dos cabeçalhos TCP/IP é feita sob dois aspectos:

a) Análise Sintática – onde é verificada a estrutura do cabeçalho, que possui como unidade básica de formação os campos; e
b) Análise Semântica – onde é verificado o significado do cabeçalho em termos dos valores dos seus campos.

Assim, para que o cabeçalho seja considerado válido é preciso que o mesmo o seja sintática e semanticamente. Ou seja, o cabeçalho deve obedecer às regras sintáticas, que determinam quais cadeias de campos podem formar cabeçalhos, e às regras semânticas, que determinam se o cabeçalho possui significado com base nos valores presentes em seus campos.

A partir do estudo e análise do conteúdo dos documentos RFCs (RFC 791, 793, 1323 e 2018) e de algumas considerações feitas acerca destes documentos em [Northcutt et al., 2001], foram definidas regras sintáticas e semânticas para os cabeçalhos IP e TCP, contabilizadas num total de trinta e uma regras.

Definidas as regras da análise sem estado, o próximo passo consiste na aplicação de um modelo lógico para criar uma teoria que corresponde ao conjunto de regras que devem ser satisfeitas para que os cabeçalhos IP e TCP sejam considerados válidos.

Aplicação de um Modelo Lógico para Formalização das Regras dos Cabeçalhos

A fim de definir logicamente as regras sintáticas e semânticas estabelecidas para os cabeçalhos IP e TCP, é construído um formalismo aplicando-se a lógica de primeira ordem. As regras dos cabeçalhos IP e TCP são interpretadas a partir da construção de uma teoria de primeira ordem. Essa teoria é formada por um conjunto de fórmulas da lógica de primeira ordem gerado a partir das regras definidas para os cabeçalhos.

Após a formalização das regras sintáticas e semânticas dos cabeçalhos, é definida, então, a fórmula principal da seguinte forma: "$\forall x \; \forall y$ (pacote_cab_val(x,y) $\leftarrow$ regras_ok(x,y))". Tal fórmula possui o seguinte significado: "x e y são, respectivamente, cabeçalhos IP e TCP válidos de um pacote se x e y atendem a todas as regras". A expressão "regras_ok(x,y)" será verdadeira se a conjunção de todas as fórmulas correspondentes às regras dos cabeçalhos forem verdadeiras. Assim, o predicado "pacote_cab_val" será utilizado para consultar se um dado conjunto de valores representa um pacote com cabeçalhos IP e TCP válidos.

Protótipo para Realização da Análise sem Estado (RECAB)

A implementação das regras que definem a validade dos cabeçalhos IP e TCP, formalizadas através de um conjunto de fórmulas da lógica de primeira ordem, é realizada utilizando-se programação em lógica.

Uma das grandes vantagens da programação em lógica, em relação à programação convencional, é que a tarefa do programador resume-se, praticamente, à especificação do problema que deve ser solucionado, visto que as linguagens lógicas podem ser vistas simultaneamente como linguagens para especificação formal e linguagens para a programação de computadores. Portanto, a teoria criada para formalizar as regras dos cabeçalhos, a qual consiste de um conjunto de fórmulas da lógica de primeira ordem, na realidade, corresponde a um programa em lógica.

Assim, o protótipo para testar as regras referentes aos cabeçalhos IP e TCP, denominado de RECAB, foi desenvolvido em Prolog. A essência do RECAB consiste na análise de pacotes individuais onde são verificadas se as regras referentes aos protocolos IP e TCP são obedecidas. Caso haja alguma violação de protocolo o pacote é identificado e os erros detectados são listados.

A fim de que os pacotes, que se encontram no formato *windump*, sejam processados pelo protótipo, é feita uma conversão dos mesmos em termos Prolog, de forma que os pacotes passam a ser representados por fórmulas atômicas [Casanova, 1987]. A idéia original, referente ao processamento dos pacotes pelo RECAB, consistia em colocar os pacotes sob análise como parte do próprio programa Prolog.

Entretanto, a fim de que o programa não ficasse sobrecarregado, comprometendo sua execução, devido ao grande número de pacotes que foram analisados, os pacotes, definidos como termos Prolog,

foram armazenados em um arquivo texto. Este arquivo, cujo conteúdo corresponde ao tráfego de rede coletado para análise, é passado como parâmetro de entrada para o RECAB, o qual faz uma leitura seqüencial do mesmo, analisando cada pacote lido, e relatando caso haja alguma violação de protocolo, até que o final do arquivo seja atingido.

3.3. Análise com Estado

Da mesma forma que na análise sem estado, o escopo da análise com estado são os cabeçalhos IP e TCP, tendo como ênfase a conexão TCP. De acordo com [Northcutt, 2000], os comportamentos mais genéricos que se pode analisar, quando o escopo é o protocolo TCP, referem-se a:

1) Estabelecimento da Conexão;
2) Transferência de Dados; e
3) Finalização da Conexão.

Seguindo esta linha base, nesta etapa que se refere à análise com estado, é proposto um esquema para estudo do comportamento da conexão TCP/IP, o ESTCON, onde será verificado se uma conexão foi estabelecida de acordo com o processo de *three-way handshake*, se houve transferência de dados após o estabelecimento da conexão, e, por fim, se a conexão foi finalizada através do uso do flag FIN ou RESET.

O ESTCON tem como foco estudar o comportamento de uma dada seqüência de pacotes, a fim de identificar quando uma situação de violação do comportamento esperado do protocolo representa algum tipo de ataque.

A implementação do ESTCON apóia-se na utilização de um banco de dados para realizar correlação de pacotes. O arquivo texto contendo os pacotes representados por termos Prolog, utilizado na análise sem estado, foi importado para o Banco de Dados Access, dando origem a uma tabela cuja estrutura é composta por todos os campos dos cabeçalhos IP e TCP. A seguir é descrito o que foi verificado no esquema proposto para realização da análise com estado, o ESTCON.

Classificação dos pacotes por Conexão

Como a análise com estado tem como foco central a conexão TCP, a primeira fase que compõe o ESTCON consiste na classificação dos pacotes de acordo com a conexão à qual eles pertencem (ou deveriam pertencer).

Essa classificação é feita através do "par socket", que consiste nos endereços de origem e destino do cabeçalho IP, e nas portas de origem e destino do cabeçalho TCP, o que identifica uma conexão de forma única na rede.

Concluída a classificação dos pacotes por conexão, agrupando-se os pacotes pelo respectivo "par socket", é iniciado um processo de verificação de quatro itens para cada conjunto de pacotes identificado como sendo uma conexão, os quais são descritos na seção seguinte.

Itens Verificados no ESTCON

A base do ESTCON consiste na verificação de quatro itens referentes aos comportamentos mais genéricos da conexão TCP/IP, definidos em [Northcutt, 2000], os quais são identificados na Tabela 1.

No item 1 é verificado se ocorreu o estabelecimento de conexão através do processo de *three-way handshake*. No item 2 é verificado se houve transferência de dados em alguma direção com a respectiva confirmação de recebimento, dentro da conexão.

No item 3 é verificado se houve solicitação de finalização de conexão através do flag FIN. Finalmente, no item 4, é verificado se o flag RST foi utilizado em algum momento dentro da conexão.

Assim, de posse dos valores obtidos nos quatro itens, pode-se identificar o que ocorreu dentro de cada conexão de acordo com a Tabela 1. Tal tabela apresenta as 16 (dezesseis) combinações possíveis referentes aos quatro itens examinados, correspondendo, dessa forma, a uma tabela-verdade dos itens do ESTCON. O conteúdo da coluna "Significado" é inferido a partir da combinação dos valores dos quatros itens, cujo objetivo maior é descrever de forma resumida o que aconteceu dentro do conjunto de pacotes analisado.

O termo "Cold Start", utilizado na Tabela 1, indica a situação em que uma conexão foi estabelecida antes do tráfego da rede começar a ser monitorado [Handley e Paxson, 2001].

Analogamente, o termo "Cold End" será utilizado com o significado de que a conexão ainda não havia sido terminada no momento em que o arquivo de log foi finalizado.

Tabela 1. Tabela-Verdade dos Quatro Itens verificados no ESTCON

	Item 1	Item 2	Item 3	Item 4		
Cód.	**Estab. de Conexão**	**Transf. de Dados**	**Flag FIN**	**Flag RST**	**SIGNIFICADO**	**STATUS**
1	V	V	V	V	Três fases completas	NORMAL
2	V	V	V	F	Três fases completas	NORMAL
3	V	V	F	V	Interrupção abrupta (possível falha de operação)	NORMAL
4	V	V	F	F	Transferência de dados não terminada (Cold End)	NORMAL
5	V	F	V	V	Inicia e finaliza conexão, sem transferência de dados	ANORMAL
6	V	F	V	F	Inicia e finaliza conexão, sem transferência de dados	ANORMAL
7	V	F	F	V	Interrupção abrupta antes de iniciar transferência de dados (possível falha de operação)	NORMAL
8	V	F	F	F	Conexão ainda não utilizada	VERIFICAR
9	F	V	V	V	Não aparece estabelecimento da conexão (Cold Start)	NORMAL
10	F	V	V	F	Não aparece estabelecimento da conexão (Cold Start)	NORMAL
11	F	V	F	V	Cold Start e término abrupto	NORMAL
12	F	V	F	F	Cold Start e Cold End	NORMAL
13	F	F	V	V	Só aparece finalização da conexão	VERIFICAR
14	F	F	V	F	Só aparece finalização da conexão	VERIFICAR
15	F	F	F	V	Resposta a pedido não aceito	VERIFICAR
16	F	F	F	F	Desconhecido	SUSPEITO

Definição de Status proposta no ESTCON

O valor de "STATUS", definido na Tabela 1, baseia-se no conhecimento do comportamento padrão dos protocolos IP e TCP, bem como em algumas técnicas de ataque que se manifestam mediante a violação de tais padrões.

O status "NORMAL" significa que o conjunto de pacotes analisado apresenta um comportamento aceitável ou esperado pelos protocolos TCP/IP. O status "SUSPEITO" significa que o conjunto de pacotes analisado apresenta um comportamento que representa uma possível forma de ataque (por exemplo, uma técnica de scan). Já o status "ANORMAL" significa que o conjunto de pacotes analisado não apresenta um comportamento padrão, não chegando, porém, a ser considerado suspeito.

Finalmente, o status "VERIFICAR" significa que somente com base nos valores dos quatro itens da tabela-verdade não é possível identificar o real status do conjunto de pacotes analisado, sendo necessário, portanto, verificar algumas questões relacionadas a seguir.

No caso do código 8 da Tabela 1, é verificado se o último pacote, presente no conjunto sob análise, localiza-se no final do log. Em caso positivo, o status da conexão é considerado "NORMAL", assumindo-se que o encerramento do log ocorreu antes do registro das fases posteriores (transferência e finalização); caso contrário, o status é dito "ANORMAL". Para efeitos do ESTCON, o posicionamento do pacote dentro do log dá-se em razão do total **N** de pacotes armazenado no mesmo, dividindo-se o log em três partes iguais (início, meio e fim), cada uma contendo (**N***33,33%) pacotes.

No caso dos códigos 13 ou 14, é verificado se o primeiro pacote, presente no conjunto sob análise, localiza-se no início do log. Em caso positivo, o status da conexão é considerado "NORMAL", assumindo-se que ocorreu "Cold Start"; caso contrário, o status é dito "ANORMAL".

No caso do código 15, que significa que dentre os quatro itens só foi constatado o uso do flag RST, primeiramente é verificado quais pacotes, dentro do conjunto sob análise, deram origem aos pacotes RST. Com base nestes pacotes, é verificado se o <End_Origem> presente nos mesmos se repete em outras "conexões" também classificadas com código 15. Caso o número de repetições ultrapasse um limiar pré-definido (valor *default* 10), o status da conexão é considerado "SUSPEITO", pois isto significa que um mesmo <End_Origem> enviou vários pacotes para diversos destinos, caracterizando um *SCAN* a partir do <End_Origem> em questão.

Caso um *SCAN* não seja configurado, é feita uma verificação da quantidade de pacotes que originaram os pacotes RST, por grupos de pacotes. Caso essa quantidade seja superior a um limiar (valor default 300), o status da conexão é considerado "SUSPEITO", configurando-se um ataque de negação de serviço (DoS) através da inundação (*FLOODING*) da porta destino com inúmeras requisições [Northcutt, 2000].

Caso um *FLOODING* não seja configurado, é verificado qual flag foi utilizado para gerar o pacote RST. Se flag=SYN, o status é considerado "NORMAL", assumindo-se que se trata de uma tentativa de conexão não aceita. Se flag=ACK, é verificado se o pacote localiza-se no início do log, caso positivo, o status é considerado "NORMAL", assumindo-se que ocorreu "Cold Start" com término abrupto, caso negativo, o status é dito "SUSPEITO", assumindo-se que houve tentativa de reconhecimento através do uso do flag ACK sem uma conexão pré-estabelecida. Por fim, se flag=FIN ou qualquer outro valor desconhecido, o status é considerado "SUSPEITO" pelo mesmo motivo de provável tentativa de reconhecimento.

4. RESULTADOS OBTIDOS

Foram realizados vários testes com o RECAB e o ESTCON envolvendo tráfego real de rede e pacotes montados contendo anomalias e simulando algumas formas de ataques. Para efeitos de comparação, os mesmos testes foram feitos com o Snort, que é um sistema de detecção de intrusão de domínio público baseado em assinaturas de ataques.

Todos os testes foram realizados em ambiente Windows 2000, com interface de rede Ethernet de 100 Mbits/sec. Foi utilizado Snort para Windows versão 1.9.1, disponível no endereço eletrônico <http://www.silicondefense.com/support/window>. A seguir são apresentados os testes realizados.

4.1. Testes com o RECAB

Como este artigo enfatiza a análise com estado, os resultados dos testes com o RECAB serão descritos de forma sucinta, ressaltando-se somente os pontos mais significativos.

O RECAB mostrou-se hábil em identificar violações de regras de protocolo, com a característica de que, a cada pacote, todas as regras eram verificadas. Esta característica permitiu a detecção de ataques que combinavam mais de uma assinatura, referentes à violação de protocolo, em um único pacote, fato este que não foi observado na análise realizada pelo Snort. Além disso, para algumas violações de protocolo o Snort sequer gerou alerta.

Entretanto, deve-se observar que o protótipo mostrou um baixo desempenho no tratamento de grandes quantidades de pacotes. Assim, há de se considerar, para uma aplicação prática, uma customização da forma de programação e, até mesmo, a utilização de outra linguagem.

4.2. Assinaturas do Snort versus Violação dos Protocolos IP e TCP

Além dos testes com o RECAB, foi feito um levantamento das assinaturas presentes no Snort, sendo verificado que poucas se referem à violação de protocolo, onde a maioria realiza buscas por strings suspeitas na parte de dados dos pacotes.

Entretanto, mesmo que para uma minoria, foi verificado que algumas regras tratadas no RECAB poderiam representar um dado conjunto de assinaturas do Snort, chegando-se numa proporção de 1:12

(uma regra para doze assinaturas). Assim, através de uma pré-análise, utilizando-se o RECAB, seria possível diminuir o número de assinaturas em um SDI, o que, dependendo da proporção, incrementaria a eficiência do mecanismo de detecção.

4.3. Testes com o ESTCON

Primeiramente, foram feitos testes com 100.000 pacotes coletados do tráfego real de uma rede TCP/IP, onde foi identificada uma situação com status "SUSPEITO", código 15 da Tabela 1. Verificou-se que a partir de um mesmo endereço de origem (host-a) foram enviados mais de 600 pacotes SYN, a 66 endereços de destino diferentes em portas diversas, tendo como resposta, por parte dos endereços de destino, na grande maioria das vezes, pacotes RST. Tal situação foi caracterizada pelo ESTCON como um *SCAN* partindo do host-a, onde o intuito seria identificar quais portas estariam ativas ou não em diversos hosts.

Entretanto, ao contactar o administrador da rede, verificou-se que o host-a correspondia a um servidor NAT (*Network Address Translation*) cujo endereço IP é utilizado por todos os hosts da rede interna para acesso à Internet. Assim, concluiu-se que não se tratava de um *scan* partindo de uma mesma origem, mas sim de vários hosts internos tentando acessar diversos destinos, gerando, portanto, um FALSO-POSITIVO.

Para testar devidamente o ESTCON, comparando-o com o Snort, foram geradas algumas seqüências de pacotes simulando ataques, utilizando-se as ferramentas *NMapWin* (www.insecure.org) e *Engage Packet builder* (www.engagesecurity.com). Os resultados são apresentados na Tabela 2.

Tabela 2. Resultados obtidos no ESTCON e no Snort referente a Pacotes Montados Simulando Ataques.

Ataque	ESTCON	Snort
Scan SYN Stealth (via NMapWin)	Scan a partir da Origem: "host-y" - Flags **SYN**, ACK, NULO, URG-PSH-FIN (Tentativas: 1616)	NMAP FINGERPRINT (stateful) STEALTH ACTIVITY (XMAS scan) STEALTH ACTIVITY (NULL scan)
Null Scan (via NMapWin)	Scan a partir da Origem: "host-y" - Flags **NULO**, ACK, URG-PSH-FIN (Tentativas: 1881)	NMAP FINGERPRINT (stateful) STEALTH ACTIVITY (XMAS scan) Gerou mais de mil alertas do tipo: STEALTH ACTIVITY (NULL scan)
ACK Scan (via NMapWin)	Scan a partir da Origem: "host-y"- Flags **ACK**, URG-PSH-FIN (Tentativas: 1876)	Gerou três alertas do tipo: STEALTH ACTIVITY (XMAS scan)
SYN-flood (via Engage Packet builder)	Denial of Service (flooding) no "host-x:porta-x" a partir da Origem: "host-y" - Flags **SYN** (Tentativas: 800)	<sem-alerta>

Ao utilizar a ferramenta *NMapWin* observou-se que ela sempre enviava em seus "*scans*" algum pacote contendo um tipo de anomalia (flag NULO ou flag ACK com <Num_Ack>=0 ou flag URG-PSH-FIN), não se restringindo a enviar pacotes com flags setados de acordo com a respectiva denominação do scan. Esses "scans" eram enviados a partir de uma origem para diversas portas em único host com o objetivo de identificar o sistema operacional rodando no host destino (*fingerprinting*). Já o ataque SYN-flood consistiu do envio de 800 pacotes SYN para uma mesma porta em um único host, com objetivo de gerar um Denial of Service (DoS) na porta de destino.

Assim, verifica-se que o Snort, apesar de ter gerado alertas para os três scans, gerou-os em decorrência dos pacotes anômalos enviados pelo *NMapWin*, os quais, na realidade, não deveriam fazer parte destes scans. Portanto, à exceção do Scan Null, conclui-se que o Snort não detectou os demais scans, nem tampouco o SYN-flood.

No ESTCON, foi atribuído status "SUSPEITO" para as quatro situações mostradas na Tabela 2. Nos três primeiros casos, foi detectado um scan a partir do "host-y", identificando-se os flags utilizados na varredura e o número de pacotes enviados, onde o flag em negrito refere-se àquele que

apareceu em maior quantidade. No caso do SYN-flood, identificou-se o destino e a origem da inundação (*flooding*), o flag utilizado e o número de pacotes enviados.

4.4. Comparação do ESTCON com um Sistema de Reconstrução de Sessões TCP/IP denominado RECON

O RECON [Chaves, 2002] é um sistema que permite reconstruir e rastrear o estado das sessões TCP/IP, utilizando o cabeçalho dos pacotes, e que implementa algumas rotinas para realizar aplicações em detecção de intrusão. Uma dessas rotinas tem o objetivo de realizar Detecção de *Host Scan* com base nas sessões reconstruídas pelo RECON, a qual foi comparada com a detecção de *scan* feita pelo ESTCON.

O RECON faz a verificação da quantidade de hosts acessados a partir de um mesmo IP utilizando uma lista de sessões TCP criada quando da análise do tráfego, onde a porta de destino tem que ser igual para todos os hosts acessados. Já no ESTCON, a mesma verificação de quantidade de hosts é feita somente onde não há sessão TCP estabelecida (código 15 da Tabela 1), não sendo necessário que a porta de destino seja a mesma, bastando somente que a "conexão" (par socket) seja diferente.

Assim, no caso de uma varredura em único host em todas as portas (1 a 65535), para saber quais serviços o mesmo oferece, o RECON não a detectaria. Já no ESTCON, mesmo o destino sendo um único host, como as portas variam, os pacotes são agrupados em "conexões" diferentes. Dessa forma, o ESTCON detectaria um scan partindo de um mesmo host com destinos diferentes.

Com relação a desvantagens, pode-se citar a questão de que o RECON também analisa sessões TCP estabelecidas na detecção de scan, o que não ocorre no ESTCON. Um exemplo de dados reais, descrito em [Chaves, 2002], apresenta uma atividade onde um mesmo host-x iniciou sessões com vários hosts na porta 25/tcp, a qual ocorreu durante 40 horas consecutivas, com picos de até 807 acessos a hosts distintos. Tal situação, que não seria detectada pelo ESTCON, foi detectada pelo RECON, sendo constatado que o host-x estava sendo explorado e utilizado para gerar SPAM.

5. CONCLUSÃO

A análise de pacotes proposta permitiu que fossem criados uma definição formal das especificações dos protocolos IP e TCP e um esquema de se fazer correlação de pacotes, que se mostraram eficientes não só para realizar detecção de alguns tipos de ataques como também para estudar o comportamento do tráfego de redes TCP/IP.

A maior vantagem observada em verificar a violação de protocolos, consiste no fato de que as possibilidades de utilização de anomalias para geração de ataques seriam esgotadas. Assim, variações de ataques e ataques desconhecidos, que envolvam violação de protocolo, poderiam ser detectados sem a pré-existência de uma assinatura.

Como trabalhos futuros, as regras do RECAB poderiam ser implementadas como um *plugin* do Snort [Roesch e Green, 2003]. Com relação ao ESTCON, poderia ser feito um estudo da taxa de falso-negativos ao se aplicar as inferências apresentadas na Tabela 1. Uma última sugestão consiste em aumentar o escopo da análise de pacotes, englobando outros protocolos, tais como ICMP e UDP.

6. REFERÊNCIAS BIBLIOGRÁFICAS

Allen, J. et al. *State of the Practice of Intrusion Detection Technologies* [online]. Pittsburgh: Carnegie Mellon University, 2000. <http://www.sei.cmu.edu/publications /documents/99.reports/99tr028/99tr028abstract.html>

Amoroso, Edward, *Intrusion Detection, An Introduction to Internet Surveillance, Correlation,TraceBack,Traps,and Response*. New Jersey:Intrudion.Net Books, 1999.

Casanova, Marco A. et al. *Programação em Lógica e a Linguagem Prolog*. São Paulo: Editora Edgard Blücher Ltda, 1987.

Chaves, Marcelo H. P. C. *Análise de Estado de Tráfego de Redes TCP/IP para Aplicação em Detecção de Intrusão*. São José dos Campos: Instituto Nacional de Pesquisas Espaciais, 2002. 172 p. (INPE-9625-TDI/845).

Handley, Mark and Paxson, Vern. *Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-end Protocol Semantics* [online]. Proc. USENIX Security Symposium 2001. <http://www.icir.org/vern/papers.html>.

Krügel, Christopher et al. *Service Specific Anomaly Detection for Network Instrusion Detection* [online]. <http://www.informatik.uni-trier.de/~ley/db/conf/sac/ sac2002.html#KrugelTK02> (2002).
Northcutt, Stephen et al. *Intrusion Signatures and Analysist´s Handbook.* Indiana: New Riders Publishing, 2001.
Northcutt, Stephen et al. *Network Intrusion Detection – An Analyst´s Handbook*. Indiana: New Riders Publishing, 2000.
Roesch, M. and Green, C. *Snort Users Manual. Release 2.0.0*. [online]. <http://www.snort.org/docs/SnortUsersManual.pdf>. Abril, 2003.

A DEFORMABLE CONTOUR BASED APPROACH FOR HAND IMAGE SEGMENTATION

Marcos Cordeiro d'Ornellas[1]

[1]Grupo de Processamento de Informações Multimídia (PIGS),
Centro de Tecnologia (CT),
Universidade Federal de Santa Maria (UFSM), Brasil

Abstract

In this paper we address the issue of hand contour segmentation from digital images using deformable contour models (snakes). We present a novel variation of the traditional snake solution, where additional nodes are inserted, and redundant nodes are deleted, to better describe the complexity of the extracted line. Node insertion and deletion are based on an analysis of the energy terms of the snake solution. This allows us to use more, closely spaced nodes along the high curvature areas of a hand, compared to the linear segments of the same hand outline. This dynamic manipulation of the number and spacing of nodes within a single snake allows us to better capture the geometry of the hand, and to better accommodate its radiometric behavior. Here we present our approach and experimental results to demonstrate its performance for hand contour segmentation as a tool for biometrics, medical imaging, and pattern recognition.

1. INTRODUCTION

In the past four decades, computerized image segmentation has played an increasingly important role in medical image processing. Image segmentation remains a difficult task, however, due to both the tremendous variability of object shapes and the variation in image quality. In particular, biometric images are often corrupted by noise and sampling artifacts, which can cause considerable difficulties when applying classical segmentation techniques such as edge detection and thresholding. As a result, these techniques either fail completely or require some kind of post-processing step to remove invalid object boundaries in the segmentation results.

To address these difficulties, *deformable models* have been extensively studied in biometric image segmentation, with promising results. Although the term *deformable models* first appeared in the work by Terzopoulos and his collaborators in the late eighties [5–7], the idea of deforming a template for extracting image features dates back much farther, to the work of Widrow's rubber mask technique [2]. Similar ideas have also been used in the work by Blake and Zisserman [1], and Grenander et al. [10]. The popularity of deformable models is largely due to the seminal paper "Snakes: Active Contours" by Kass,Witkin, and Terzopoulos [9]. Since its publication, deformable models have grown to be one of the most active and successful research areas in image segmentation. Various names, such as snakes, active contours or surfaces, balloons, and deformable contours or surfaces, have been used in the literature to refer to Image Segmentation Using Deformable Models.

The paper is organized as follows. In Section 2 we present an overview of the traditional snake solution, focusing on the relevant energy terms. In Section 3 we present our approach for the dynamic positioning of snake nodes using by analyzing the snake energy terms. Experimental results are presented in Section 4 to demonstrate the performance of our approach for hand contour extraction in biometric applications. We conclude with comments in Section 5. It should be noted that we focus on describing the fundamentals of deformable models and their application to hand image segmentation. Treatment of related work using deformable models in other applications such as image registration and motion estimation is beyond the scope of this chapter.

2. SNAKE MODEL

2.1. Energy Functions

In general, the energy function of a snake contains descriptions of internal and external forces, as well as external constraints. The internal forces allow the contour to stretch or bend at the specific point, while maintaining certain smoothness and continuity. The external force attracts the contour to significant features on the image (namely the hand location in it), while the external constraints represent user-imposed restrictions. The total energy of each point is expressed as a sum of individual energy terms:

$$E_{snake} = \alpha E_{cont} + \beta E_{curv} + \gamma E_{edge}$$

where E_{cont} and E_{curv} are the first and second order continuity constraints (internal snake forces), E_{edge} is the edge strength (external snake force), and α,β, and γ are relative weights of each energy term. Internal forces tend to produce smooth snake curves, while the external forces attract the snake to edge locations in the image.

2.2. Continuity Term

If $v_i(x_i,y_i)$ is a point on the contour, the first energy term in the total energy function is defined as follows:

$$E_{cont} = d_{av} - \left| v_i - v_{i-1} \right|$$

with d_{av} being the average distance between points, defined for a snake with n points as:

$$d_{av} = \sum_{i=1,n-1} \left| v_{i+1} - v_i \right| / (n-1)$$

The continuity energy term guarantees that snake points will be evenly spaced, while minimizing their distance.

2.3. Curvature Term

This is an estimation of the snake's second derivative and is calculated as:

$$E_{curv} = \left| v_{i-1} - 2v_{i-1} + v_{i+1} \right|^2$$

Since the continuity term produces evenly spaced points, the above term gives the snake curvature multiplied by a constant. This constant becomes insignificant, because the curvature term is normalized in the neighborhood of each point.

2.4. Edge Term

This energy term describes the external force that attracts the snake to the hand location in the image. In general, it forces points to move towards image edges. An expression of this term may be provided by:

$$E_{edge} = -\nabla I(v_i)$$

where $I(v_i)$ is the image function (gray values) at snake point v_i. We use the negative sign to attract the snake to image points with high gradient values [3-4]. Since the gradient is a metric for image edges, the snake is attracted to strong edge points. The image gradient at each point is normalized to handle even small gray value variations at the neighborhood of that point.

2.5. Optimization Procedure

After the initialization of the snake contour, the points along the contour move to new energy minimum locations. These new locations are found through an iterative procedure. In any iteration, an optimization process is used to compute the new snake location. An alternative, approach is suggested in [8]. This method (greedy algorithm) is found to be faster than dynamic programming and more stable and flexible than the variational calculus approach. This is the method used in our implementation of snakes.

3. PROPOSED METHOD

3.1. Fundamentals

Our main objective is to improve the accuracy of hand extraction by selectively intensifying the interpolation resolution. By having nodes equally distributed, common snakes solutions do not take into account the geometric complexity of the extracted object. This lowers the accuracy of the extracted representation. In hand extraction this is commonly manifested by extracting a polygonal approximation that deviates from the actual hand by few pixels. To overcome such problems we propose an adaptive iterative snake solution where the snake solution of iteration is analyzed to:

- Remove redundant nodes;
- Enhance locally the solution as necessary, to better capture the geometric complexity of the extracted feature.

Our argument is that the quality of the snake solution is inherently described by the local values of its corresponding energy terms. More specifically, the output result of a snake solution includes the optimized coordinates of snake nodes, the energy values of each point and its components (continuity, curvature and edge). These energy components indicate how well the snake has performed on each point. The general flowchart of the proposed method is shown in figure 1.

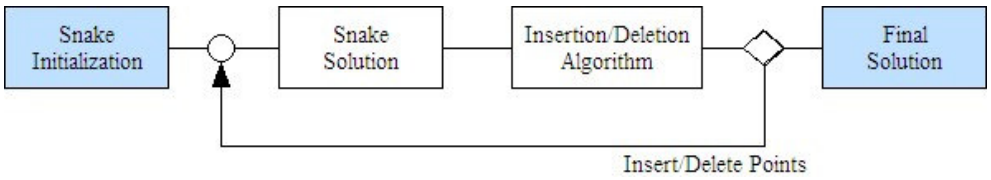


Figure 1: General Flowchart of the approach presented in this paper.

3.2. Node Detection

The flowchart of this operation is shown in figure 2. The purpose of node *deletion* is to improve the efficiency of hand extraction by removing redundant points without lowering the extraction accuracy. In order to achieve this we set the following rules for node deletion (assuming the gradient values): the radiometric information is good, *and* the curvature term is very low.

The first condition states that there is a great probability that this point belongs on the hand edge. Good gradient is implied from (absolute) high edge term (equation 5). If E_{edge} is the radiometry term, we define the threshold for good radiometry (E_{edge}ThrHigh) as:

$$E_{edge}ThrHigh = \min\left(E_{edge}\right) + range\left(E_{edge}\right) * EnHigh$$

Points that have E_{edge} greater than E_{edge}ThrHigh are considered to have good gradient and are candidates for deletion.

The second rule guarantees that the geometry of the snake will be distracted minimally. The smoothness of the snake is described in the curvature term. If the curvature of the point is low, it implies that the snake is very smooth (close to straight line) in that area. If E_{curv} is the curvature term, we define the threshold for low curvature (E_{curv}ThrLow) as:

$$E_{curv}ThrLow = \min\left(E_{curv}\right) + range\left(E_{curv}\right) * EnLow$$

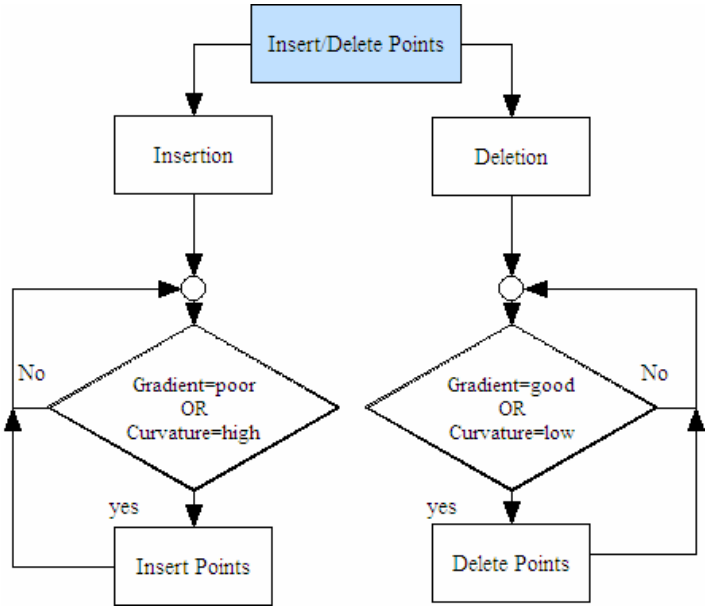


Figure 2: Deletion and Insertion Flowchart

If any points have E_{curv} lower than E_{curv}ThrLow, they are candidates for deletion, as their curvature is very low. Finally, we combine the above two rules and we select the candidate points that satisfy these rules, for deletion. Note that we demand both of the rules to be true for point deletion. The next step is to insert points between the remaining snake points.

3.3. Node Insertion

The flowchart of this operation is presented in figure 2. The objective of this operation is to improve the accuracy of object extraction by inserting additional nodes in areas where the snake has not performed well or in areas where the snake resolution was not sufficient to follow the actual hand curvature. In those areas we increase the snake resolution by adding more points. The rules for point insertion are the following: the radiometry is poor, *or* the curvature is high.

The first condition is necessary for areas where there are gaps in the continuity of the hand. As in the previous subsection, poor radiometry is implied from low edge term. The threshold for poor radiometry is the same (E_{edge}ThrHigh) as in the previous equation. This time we consider points that have E_{edge} lower than E_{edge}ThrHigh as candidates for point insertion.

The second condition is needed in the areas where the snake resolution is not large enough to follow the curvature of the hand. In those areas the curvature of the snake is high. Similarly to the last equation we define the threshold for high curvature (E_{curv}ThrHigh) as:

$$E_{curv}ThrHigh = \min(E_{curv}) + range(E_{curv}) * EnHigh$$

If any points have E_{curv} higher than E_{curv}ThrHigh, they are candidates for insertion, as their curvature is very high. In case that anyone of those criteria is satisfied, then two additional points are inserted; one on each side of the point under investigation by interpolating the specific point coordinates with each one of its neighbors. As previously indicated, our approach makes use of the energy thresholds EnHigh and EnLow. These thresholds can be defined by a user, or they may be selected automatically through a statistical analysis of the snake solution data.

4. EXPERIMENTAL RESULTS

The approach described in this paper has been implemented in using Matlab. In order to evaluate the performance of the proposed approach, we need to define a quality index for the accuracy of the extraction. For each line segment (N_i-N_{i+1}) between neighboring snake points (figure 3), we identify the midpoint (M_i). Next, we calculate the distance (d_i) of this midpoint (M_i) from the hand and we define the quality index (Q) as the mean of all these distances:

$$Q = \sum_{i=1,n-1} d_i / (n-1).$$

The units of Q are pixels. Smaller values of Q indicate a snake solution closer to the true hand, and therefore indicate better solutions.

The analysis of the results was performed using Matlab tools. For the image windows shown in Figures 3-5 we performed the proposed snake solution to extract the indicated hand segments. The solution in figure 5 made use of 28 snake nodes, and the corresponding quality index was Q_0=1.1.

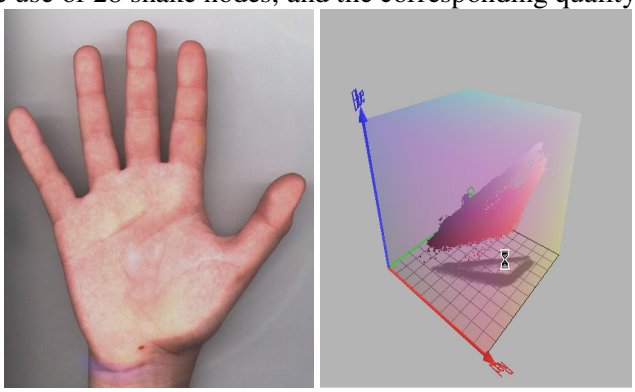


Figure 3: A RGB image of a hand and its related RGB 3D distribution histogram. Note that the uneven illumination in the hand image is reduced by using a morphological pre-processing.

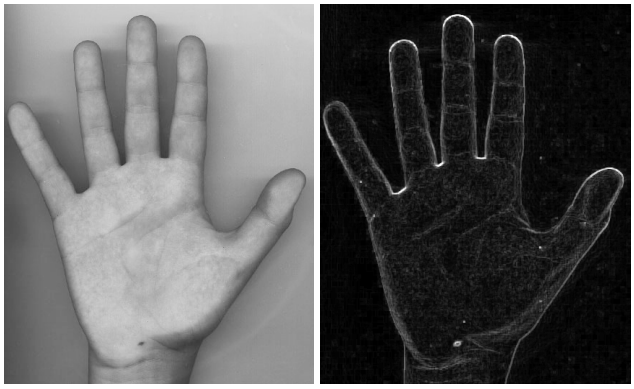


Figure 4: Grayscale version of the hand image in figure 3 and its morphological gradient.

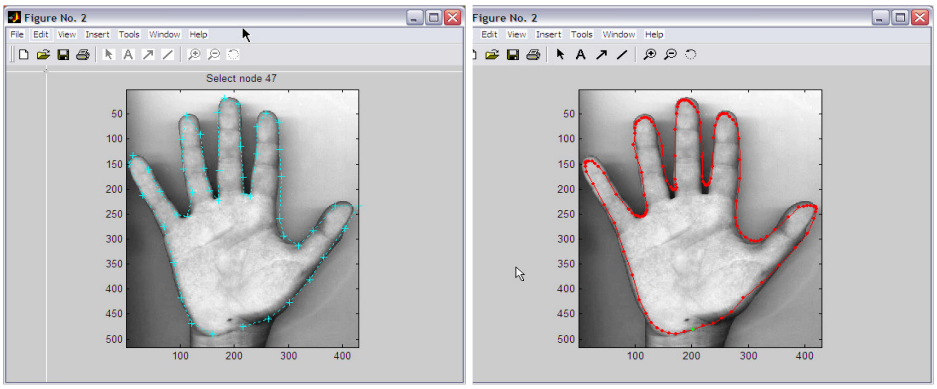


Figure 5: Point insertion and deletion and an image sample from the iterative snake approach.

Similar experiments have been performed with several images and hand segments. The results used to demonstrate the performance of our approach in this paper are representative of an average solution.

5. CONCLUSION

In this paper we presented a new method for improving hand extraction accuracy using snakes for biometric purposes. Our approach is based on an iterative application of snakes, where additional nodes are inserted, and redundant nodes are deleted, to better describe the complexity of the extracted

line. This dynamic manipulation of node distribution is based on an analysis of the energy terms of the snake solution.

The algorithm is a promising tool for the analysis of hand images for biometric and security purposes. It will provide experts with a tool for measurement and physical interpretation of deformation in hand images, and can thus be of great aid in the interpretation and indexing of these images through metadata.

6. REFERENCES

[1] A. Blake and A. Zisserman, *Visual Reconstruction*. Boston: MIT Press, 1987.
[2] B. Widrow, "The "rubber-mask" technique," *Pattern Recognition*, vol. 5, pp. 175– 211, 1973.
[3] C. Xu and J. L. Prince, "Generalized gradient vector flow external forces for active contours," *Signal Processing—An International Journal*, vol. 71, no. 2, pp. 131–139, 1998.
[4] C. Xu, D. L. Pham, M. E. Rettmann, D. N. Yu, and J. L. Prince, "Reconstruction of the human cerebral cortex from magnetic resonance images," *IEEE Trans. Med. Imag.*, vol. 18, pp. 467–480, 1999.
[5] D. Terzopoulos, "On matching deformable models to images." Technical Report 60, Schlumberger Palo Alto research, 1986. Reprinted in *Topical Meeting on Machine Vision*, Technical Digest Series, Vol. 12, 1987, 160-167.
[6] D. Terzopoulos and K. Fleischer, "Deformable models," *The Visual Computer*, vol. 4, pp. 306–331, 1988.
[7] D. Terzopoulos, A. Witkin, and M. Kass, "Constraints on deformable models: recovering 3D shape and nonrigid motion," *Artificial Intelligence*, vol. 36, no. 1, pp. 91–123, 1988.
[8] L. D. Cohen, "On active contour models and balloons," *CVGIP: Imag. Under.*, vol. 53, no. 2, pp. 211–218, 1991.
[9] M. Kass, A. Witkin, and D. Terzopoulos, "Snakes: active contour models," *Int'l J. Comp. Vis.*, vol. 1, no. 4, pp. 321–331, 1987.
[10] U. Grenander, Y. Chow, and D. M. Keenan, *Hands: A Pattern Theoretic Study of Biological Shapes*. New York: Springer-Verlag, 1991.

FORENSE COMPUTACIONAL COM SLEUTH KIT + THE AUTOPSY FORENSIC BROWSER

Ricardo Kléber Martins Galvão

NARIS – Núcleo de Atendimento e Resposta a Incidentes de Segurança
Superintendência de Informática – Gerência de Redes
Universidade Federal do Rio Grande do Norte – UFRN
http://naris.info.ufrn.br - rk@ufrnet.br

Abstract

With the significant increase of the number of machines invaded with data (logs) extinguished for the invader, as well as of the necessity of skill in machines used for the practical one of other electronic delicts, the tools of forensic computational have a vital paper in the auditorship of mass devices, mainly in that it refers to the recovery and identification of content of the extinguished data. For the inquiry of UNIX-Like machines the TCT - The Coroner's Toolkit has been used successfully. With the limitation of this solution to the auditorship of partitions UNIX of course appears the necessity of similar tools, however, that they investigate other types of systems of archives. The set of tools presented in this article supplies this lack recognizing and investigating partitions NTFS, FAT, UFS, EX2 and EXT3, generating reports detailed in an browse, beyond resources adds to already implemented for the TCT.

1. INTRODUÇÃO

1.1. Forense com o TCT

A utilização das ferramentas do TCT (unrm + lazarus) para a investigação de blocos livres em partições EXT2 apresenta como grande atrativo a visualização dos dados via browser com *hiperlinks* indicando o provável tipo de arquivo recuperado tendo a legenda (letra → tipo de arquivo) como descrito na Figura1.

Letra	Descrição	Letra	Descrição
A	Arquivo	Q	Mailq
C	Código C	R	Removido
E	ELF	S	LISP
F	Sniffers	T	Texto
H	HTML	U	Uuencoded
I	Imagem	W	Arquivo passwd
L	Logs	X	Exe
M	Mail	Z	Comprimido
O	Null	.	Binário
P	Programas	!	Som

Figura1 – Legenda do relatório apresentado pela ferramenta TCT/Lazarus

A coleta de dados, feita com a ferramenta **unrm**, é simples, bastando informar o *device* (dispositivo) a ser investigado e o arquivo para onde será gerada a imagem dos blocos não alocados, como no exemplo da Figura2 em que um hd IDE investigado é montado como *slave* (secundário) e sua primeira partição é investigada (hdb1).

```
unrm /dev/hdb1 >> imagem_hd.out
```

Figura2 – Exemplo de coleta de blocos não alocados com a ferramenta TCT/unrm

A imagem é então submetida à ferramenta Lazarus – como exemplificado na Figura3 – que a interpreta para gerar os arquivos HTML visualizados a partir de qualquer *browser*, como na Figura5.

```
lazarus -h -D . -H . -w . imagem_disquete.out
```

Figura3 – Exemplo de utilização da ferramenta TCT/Lazarus para geração de visualização via browser

Os principais parâmetros utilizados pelo Lazarus estão descritos na Figura4.

-h cria um documento HTML (visualizado por qualquer *browser*);
-D <dir> direciona a escrita dos blocos para um diretório específico;
-H <dir> direciona os principais arquivos HTML para um diretório específico;
-w <dir> direciona outras saídas HTML para um diretório específico.

Figura4 – Principais parâmetros utilizados pelo TCT/Lazarus

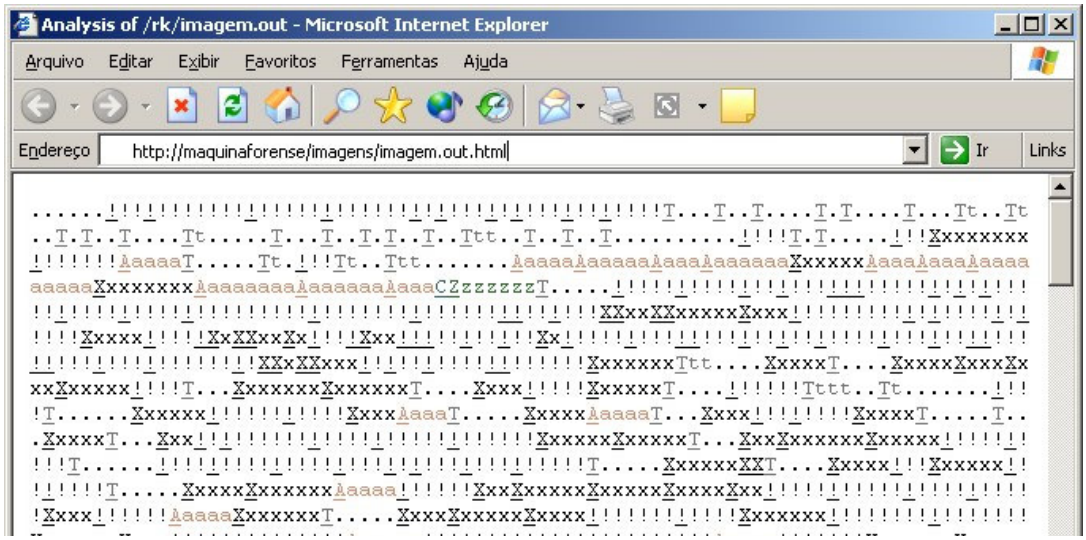


Figura5 – Exemplo de visualização via browser de um resultado gerado pelo TCT/Lazarus

Análise do TCT

Analisando criticamente o TCT e suas ferramentas **unrm** e **Lazarus**, dois fatores contribuem negativamente para a sua eficiência plena e adoção como solução principal para a auditoria de sistemas com dados apagados:

a) Limitação do tipo de partição investigada

As ferramentas do TCT não reconhecem partições NTFS, FAT e EXT3, inviabilizando a perícia em máquinas com sistemas operacionais Microsoft Windows e/ou sistemas operacionais Linux com sistema de arquivos EXT3.

As novas funcionalidades do EXT3 quando comparado ao EXT2 têm feito com que administradores prefiram este sistema de arquivos e, assim, diminuam cada vez mais o universo de máquinas passíveis de investigação com as ferramentas do TCT.

Apesar do grande avanço na utilização do sistema operacional Linux, principalmente no âmbito dos servidores, o número de máquinas com o Microsoft Windows ainda é muito grande entre os servidores e maior ainda quando leva-se em consideração o mercado de desktops.

A investigação de partições Windows (FAT) com o TCT somente é possível com a conversão para o formato EXT2, exigindo a alteração da tabela de i-nodes da partição investigada, condição nem sempre possível em se tratando de análise de dados.

b) Interface web pouco amigável

Apesar das legendas e da utilização de cores para identificar os tipos de blocos encontrados pelo Lazarus (ver Figura5), a interface deixa a desejar já que presume o conhecimento da legenda e não fornece dados adicionais sobre os dados.

2. SLEUTH KIT + THE AUTOPSY FORENSIC BROWSER

2.1. Sleuth Kit[1]

O Sleuth Kit é um conjunto de ferramentas *open source* para forense digital desenvolvido por Brian Carrier para utilização em sistemas UNIX (Linux, OS X, FreeBSD, OpenBSD e Solaris) e capaz de analisar sistemas de arquivo NTFS, FAT, UFS, EXT2 e EXT3.

Em sua primeira versão o Sleuth Kit era chamado de The @stake Sleuth Kit (TASK) e consiste em uma coleção de comandos baseados em linha de comando baseada no TCT.

Com este kit pode-se examinar sistemas de arquivos de computadores suspeitos utilizando uma abordagem não-intrusiva que independe do sistema operacional da máquina investigada para processar o sistema de arquivos, arquivos apagados e ocultos de partições DOS, BSD, Mac, Sun e Linux.

Os resultados gerados pelas ferramentas do Sleuth Kit são então utilizadas por outra ferramenta – The Autopsy Forensic Browser[2] – que exibe através de uma interface gráfica detalhes sobre a partição investigada como integridade de imagem, busca por palavras-chave e outras operações automatizadas.

Características Relativas a Entrada de Dados

- O Sleuth Kit analisa imagens de sistemas de arquivos geradas pelo comando **dd** – encontrado em todos os UNIX e também disponível para Microsoft Windows – em formato não-proprietário;
- O formato de dados da partição investigada (NTFS, FAT, UFS, EXT2 ou EXT3) não depende do sistema operacional em uso na máquina em que o Sleuth Kit está sendo executado;
- O Sleuth Kit pode ser executado a partir de um sistema UNIX durante a resposta a um incidente, exibindo arquivos que porventura estejam sendo escondidos por rootkits em execução sem modificar os arquivos (nem mesmo o A-Time) que estão sendo investigados.

Técnicas de Busca

- Listagem dos nomes de arquivos apagados e alocados;
- Exibição dos detalhes e do conteúdo de todos os atributos NTFS (inclusive Alternate Data Streams);
- Exibição de detalhes do sistema de arquivos e estrutura de meta-dados;
- Criação de linhas de tempo de atividade dos arquivos, podendo, inclusive, ser importados por planilhas para a criação de gráficos e relatórios;
- Visualização de arquivos hash em uma base de dados de hashes, customizando bases de dados que podem ser criadas com a ferramenta md5sum;

[1] http://www.sleuthkit.org
[2] http://www.sleuthkit.org/autopsy

- Organização de arquivos com base em seus tipos (separando, por exemplo, executáveis, imagens e documentos), podendo gerar pequenas imagens (*thumbnails*) a partir das imagens encontradas para uma análise mais rápida.

Características Gerais

O Sleuth Kit foi escrito em C e em Perl e utiliza parte do código do TCT, tendo sido testado em plataformas Linux, Mac OS X, Open & FreeBSD, Solaris e CIGWIN.

As informações deste artigo referem-se à versão 1.70 de 02 de Junho de 2004. Existem, ainda, na página do projeto extensões (Add-ons) que podem ser aplicadas sob a forma de *patch* para "incrementar" determinadas funcionalidades do Sleuth Kit como por exemplo para a exibição de nomes Unicode em partições NTFS e a indexação de imagens por nomes.

Detalhes sobre as Ferramentas do Sleuth Kit

- Ferramentas para Sistemas de Arquivos: Realizam o processamento geral de dados dos sistemas de arquivos, como layout e estruturas de alocação.
  - **fstat**[3]**:** Exibe detalhes do sistema de arquivos e estatísticas, incluindo layout, tamanho e labels.
- Ferramentas para Nomes de Arquivos: Realizam o processamento da estrutura de nomes de arquivos, tipicamente localizados em diretórios pais.
  - **ffind**[4]**:** Busca nomes de arquivos alocados e não-alocados a partir de um ponto na estrutura de metadados;
  - **fls**[5]**:** Lista nomes de arquivos e diretórios em uma imagem analisada.
- Ferramentas para Metadados: Realizam o processamento de estrutura de metadados armazenando detalhes sobre os arquivos.
  - **icat**[6]**:** Extrai as unidades de dados de um arquivo, especificado por um endereço de metadados (número de i-node);
  - **ifind**[7]**:** Busca por estrutura de metadados;
  - **ils**[8]**:** Lista a estrutura de metadados e seu conteúdo em um formato delimitado por pipes;
  - **istat**[9]**:** Exibe as estatísticas e os detalhes sobre a estrutura de metadados (i-nodes) em um formato de fácil entendimento.

- Ferramentas para Unidades de Dados: Realizam o processamento das unidades de dados onde o conteúdo dos arquivos estão armazenados (clusters FAT e NTFS e blocos/fragmentos em UFS, EXT2 e EXT3).
  - **dcat**[10]**:** Extrai o conteúdo de uma unidade de dados;
  - **dls**[11]**:** Lista detalhes sobre unidades de dados e pode extrair o espaço não-alocado de um sistema de arquivos;
  - **dstat**[12]**:** Exibe as estatísticas sobre uma unidade de dados em um formato de fácil leitura;

[3] http://www.sleuthkit.org/sleuthkit/man/fsstat.html
[4] http://www.sleuthkit.org/sleuthkit/man/ffind.html
[5] http://www.sleuthkit.org/sleuthkit/man/fls.html
[6] http://www.sleuthkit.org/sleuthkit/man/icat.html
[7] http://www.sleuthkit.org/sleuthkit/man/ifind.html
[8] http://www.sleuthkit.org/sleuthkit/man/ils.html
[9] http://www.sleuthkit.org/sleuthkit/man/istat.html
[10] http://www.sleuthkit.org/sleuthkit/man/dcat.html
[11] http://www.sleuthkit.org/sleuthkit/man/dls.html
[12] http://www.sleuthkit.org/sleuthkit/man/dstat.html

- **dcalc**[13]**:** Calcula onde os dados em uma imagem de espaços não-alocados (geradas a partir de um dls) estão localizados na imagem original. Esta ferramenta é utilizada quando uma evidência é encontrada em um espaço não-alocado.

- Ferramentas para Gerenciamento de Mídias: Estas ferramentas tomam a imagem de um disco (ou de outras mídias) como entrada e analisam a estrutura de gerenciamento em que estão organizados.
  - **mmls**[14]**:** Exibe o layout de um disco, incluindo espaços não-alocados. A saída identifica o tipo de partição e seu tamanho, de modo a facilitar a utilização do **dd** para extrair as partições. A saída é classificada baseando-se no setor de inicialização de modo a facilitar a identificação no layout.
- Outras Ferramentas
  - **hfind**[15]**:** Usa um algoritmo de classificação binária para localizar hashes;
  - **mactime**[16]**:** Utiliza como entrada o resultado das ferramentas fsl e isl para criar uma linha de tempo de atividade de um arquivo;
  - **sorter**[17]**:** Classifica arquivos baseando-se em seu tipo de arquivo e executa a checagem de extensões e verificação de bases de dados hash.

2.2. The Autopsy Forensic Browser

Esta ferramenta *Open Source* escrita em Perl provê uma interface gráfica para o Sleuth Kit baseada em HTML semelhante a um gerenciador de arquivos, exibindo detalhes sobre dados apagados e estruturas de sistemas de arquivos, cujo resultado pode ser acessado de qualquer plataforma utilizando um browser HTML.

Ao contrário do Lazarus, o Autopsy não necessita que nenhuma ferramenta seja executada anteriormente, podendo trabalhar diretamente sobre partições montadas ou sobre arquivos de imagem gerados com o aplicativo **`dd`**.

O Autopsy pode ser considerado somente uma interface gráfica do Sleuth, já que todos os procedimentos realizados em sua interface geram comandos do Sleuth Kit que são interpretados e exibidos novamente pelo Autopsy.

A execução é simples. Após instalado, basta executar o binário **`autopsy`** que indicará o endereço/porta para ser acessado via browser. Estes dados podem ser padronizados no arquivo de configuração do Autopsy.

Funcionalidades Adicionais

Ao ser executado, o Autopsy solicita a criação de um novo **`Case`** ou a abertura de um **`Case`** pré-existente. Cada **`Case`** criado é armazenado sob a forma de diretório para facilitar a busca por auditorias feitas com o Autopsy.

Dentro de cada Case deve-se especificar um ou mais **`Hosts`** que serão sub-diretórios dos **`Cases`** especificando, por exemplo, auditorias em mais de uma máquina em um mesmo processo.

Depois disso todos os menus apresentam funcionalidades do Sleuth Kit que será invocado a cada solicitação na interface web.

---

13 http://www.sleuthkit.org/sleuthkit/man/dcalc.html
14 http://www.sleuthkit.org/sleuthkit/man/mmls.html
15 http://www.sleuthkit.org/sleuthkit/man/hfind.html
16 http://www.sleuthkit.org/sleuthkit/man/mactime.html
17 http://www.sleuthkit.org/sleuthkit/man/sorter.html

3. EXECUTANDO O SLEUTH KIT + THE AUTOPSY FORENSIC BROWSER A PARTIR DE UM CD

Na maioria dos procedimentos de auditoria de máquinas suspeitas e/ou comprometidas, o trabalho pericial deve ser feito sem retirar o disco rígido. Como não pode-se confiar no sistema operacional da máquina analisada, recomenda-se autilização de um 'live-cd' preparado para esta tarefa, ou seja, um CD bootável com as ferramentas básicas do UNIX presentes juntamente com o Sleuth Kit e o Autopsy e outras ferramentas de auditoria.

Algumas distribuições já disponibilizam CDs com este perfil (imagens .ISO) facilitando o trabalho pericial. Duas delas são apresentadas a seguir:

- Professional Hackers Linux Assault Kit (http://www.phlak.org)
  Distribuição derivada do Morphix, criada por Alex de Landgraaf.
- Knoppix security tools distribution (http://www.knoppix-std.org)
  Distribuição baseada no consagrado Knoppix com gerenciadores de janelas leves, ideal para perícia em máquinas mais antigas.

4. REFERÊNCIAS BIBLIOGRÁFICAS

CARRIER, Brian. The Sleuth Kit & Autopsy: Forensic Tools for Linux and other Unixes.Disponível *online* em julho de 2004 na URL http://www.sleuthkit.org.

CARRIER, Brian. File System Analysis Techniques. Disponível *online* em julho de 2004 na URL http://www.sleuthkit.org/sleuthkit/docs/ref_fs.html.

CARRIER, Brian. File Activity Timelines. Disponível *online* em julho de 2004 na URL http://www.sleuthkit.org/sleuthkit/docs/ref_timeline.html.

CARRIER, Brian. The FAT File System – Sleuth Kit Implementation Notes (SKINs). Disponível *online* em julho de 2004 na URL http://www.sleuthkit.org/sleuthkit/docs/skins_fat.html.

CARRIER, Brian. The NTFS File System – Sleuth Kit Implementation Notes (SKINs). Disponível *online* em julho de 2004 na URL http://www.sleuthkit.org/sleuthkit/docs/skins_ntfs.html.

CARRIER, Brian. The Sleuth Kit Informer – Issue #13 - UNIX Incident Verification with Autopsy. Disponível *online* em julho de 2004 na URL http://www.sleuthkit.org/informer/sleuthkit-informer-13.txt.

LUCAS, Charles. Running Sleuthkit and Autopsy Under Windows. Disponível *online* em julho de 2004 na URL http://www.memophage.net/Running_Sleuthkit_and_Autopsy_Under_Windows.pdf.

LEVANTAMENTO DO HISTÓRICO NA CENA DO CRIME, FATOR RELEVANTE NA ANÁLISE DE EVIDÊNCIAS EM CRIMES ELETRÔNICOS

Erica Rocha Lima

Resumo

Este trabalho tem como objetivo apresentar o que já existe em outros países em relação à padronização e uso de metodologias na Ciência da Forense Computacional. Como deram início aos trabalhos, criação dos órgãos regulamentadores e como o Brasil encontra-se em relação a estes estudos.

Dentre os processos sobre a Evidência no ramo desta ciência, será citada neste trabalho as metodologias e passos a seguir sobre o levantamento do histórico na cena do crime, e o que este pode auxiliar durante a análise das evidências coletadas.

1. INTRODUÇÃO

Internet, rede de computadores e automação de sistemas tornaram-se grandes oportunidades em potencial para atividades criminais. Computadores e outros dispositivos eletrônicos estão sendo usados nos crimes eletrônicos cometidos contra pessoas e organizações. Evidências eletrônicas ficam registradas nos computadores ou nos sistemas que sofreram o ataque e ou nos que permitiram o crime.

Como se estivesse montando um jogo de quebra-cabeça o perito levantará as hipóteses. Juntando a cena do crime, as evidências colhidas, analisadas e tratadas, tentará compor um material necessário, as provas, que iniciarão o processo judicial.

Hoje em dia no Brasil, sabe-se pouco sobre como estruturar este quebra-cabeça. Procedimentos, referências e regras, indicadores de que passos seguir para montar o quebra-cabeça ainda são rudimentares.

Sob a visão deste problema já notificado (GEUS, 2001), abordarei os benefícios decorrentes ao usar metodologias mostrando a importância do levantamento do histórico auxiliando o perito dentro do processo de confecção e montagem deste quebra-cabeça.

2. RETRATO DA SITUAÇÃO ATUAL

A importância em se padronizar a Ciência Forense é citada como unanimidade nas literaturas pesquisadas.

Aprender com o fator sucesso e também com as notificações de limitações encontradas e dificuldades são informações de grande valor para fundamentar as hipóteses e nortear um trabalho que está se iniciando. Para analisar o problema com mais detalhes e apresentar o que já existe, vamos dar uma passeada na terra do "Tio Sam", abordando informações históricas em ordem cronológica.

É no exterior (NIJ GUIDE, 2001), e principalmente nos Estados Unidos, onde feliz ou infelizmente encontra-se não toda, mas a grande parte da literatura sobre Forense Computacional. Os laboratórios do FBI-USA estão desde aproximadamente 1984 pesquisando e desenvolvendo programas sobre evidências em computadores. Para especificar sobre o crescimento da demanda de investigadores e promotores de justiça em estruturar, o FBI fundou o CART (Computer Analysis and Response Team). Em 1991, já com o termo Forense Computacional foi criada a primeira sessão de treinamento auxiliado pelo IACIS (International Association of Computer Specialist).

Em maio de 1998, os órgãos NCTP (National Cybercrime Training Partnership), OLES (Office of Law Enforcement Standarts) em conjunto com o NIJ (National Institute of Justice) colaboraram com recursos a serem implementados contra o crime eletrônico. As iniciativas de se chegar a um denominador em comum e auxiliar nos crimes eletrônicos contra pessoas e instituições, não foram exclusivas dos órgãos que regulamentam estas modalidades de crimes (IACIS e OLES), mas também estavam presentes os que regulamentam e efetivam as leis (NIJ).

Eles não pararam por aí, continuaram se reunindo para criar e formular uma série de protocolos que listam os processos de evidências eletrônicas da cena de um crime. Sob estes documentos foi gerado um modelo, que seria o caminho para gerar os produtos elaborados e permitir novas publicações. O NIJ criou o TWGCSI (Technical Working Group for Eletronic Crime Scene Investigation), que tem a finalidade de identificar, definir e criar critérios básicos para auxiliar com investigações eletrônicas e promotores de justiça.

Em 1999, no primeiro encontro do TWGCSI, se deliberou que o processo de padronização seria desenvolvido por grupos temáticos. Foram definidos os seguintes grupos: Dispositivos de Evidências: Tipos e Evidências em Potencial; Ferramentas para Investigação e Equipamentos; Segurança e Avaliação da Cena; Documentação da Cena; Coleta da Evidência; Empacotamento, Transporte e Armazenamento; e Exame Forense por Categoria de Crimes. Em outros encontros do TWGCSI foi possível preparar o volume deste documento. Baseando-se nas alterações e inovações das cenas dos crimes, foi possível comparar com o que já existia do projeto elaborado e revisá-lo. Por fim, aos anos 2001 foi elaborado um Guia para Primeiras Respostas nas investigações das Cenas em Crimes Eletrônicos.

O processo, que está em contínuo desenvolvimento, não terminou em 2001, porém esse breve histórico permite mostrar os caminhos seguidos, os órgãos envolvidos, o que foi pesquisado e os esforços empreendidos para a especificação e criação de regras. A forma de condução deste trabalho realizado nos Estados Unidos, o que foi feito para chegar à estruturação e à elaboração de regras e referências é um excelente exemplo para se dar início às especificações de procedimentos, protocolos de investigações, classificação e, porque não mencionar, a criação de uma Metodologia a ser adotada.

Sebadash (2004) cita em seu documento métodos e práticas de investigação e ressalta a forma de classificação das vítimas, que sofrem ataques de crimes eletrônicos: proprietários dos sistemas com 79%, seus clientes com 13% e 8% com os terceiros. Em uma análise quantitativa são apresentadas as vítimas proprietárias dos sistemas que não notificam os incidentes e quais as razões possíveis desta posição. Entre outros fatores, encontra-se o de não confiar na política que irá investigar e o próprio cuidado de não deixar vazar tal informação por proteção aos seus negócios. De acordo com os fatos e acontecimentos relatados, é possível um estudo dos especialistas nas novas modalidades de crimes, podendo prestar um atendimento às empresas com mais qualidade nas investigações.

Num dos primeiros trabalhos de especificação das normas para as análises computacionais forense, nossos vizinhos argentinos (GOMEZ, 2002), os processos a serem adotados durante a investigação de um crime eletrônico. A metodologia proposta é estruturada em quatro segmentos claramente definidos: a classificação das atividades, as relações dos alinhamentos e dos procedimentos de armazenamento das evidências, as análises dos dados colhidos e a capacitação do perito em órgãos internacionais certificadores tais como o IACIS e HTCN (High-Tech Crime Network). O documento possui clareza e objetividade no que se refere à estruturação e organização para o início da criação das normas.

O Brasil ainda não dispõe de vasta literatura sobre as práticas da Forense Computacional. Porém, as publicações existentes mostram a iniciativa em se abordar esse segmento de grande amplitude e estruturá-lo cientificamente, atendendo as necessidades tecnológicas e judiciais para tratamento dos incidentes. Atualmente dispomos de um mapeamento sobre a realidade do que já existe e do que é necessário ser feito.

Sendo Geus (2001), é importante desenvolver procedimentos e protocolos detalhados para suportar os resultados de uma análise forense, desde que estes sejam de documentos revisados, aceitos pela comunidade científica e que assegurem requisitos legais e técnicos à prova pericial, ou seja, que sejam válidos e confiáveis para a recuperação e utilização das evidências digitais. Devem ser desenvolvidas novas técnicas para a abordagem dos crimes e a obtenção das evidências armazenadas nos computadores.

Acredito, que este é o caminho a ser seguido, criar tais procedimentos e padrões, de forma semelhante ao que fizeram os outros países. Serão necessários a avaliação e o desenvolvimento dos procedimentos, que serão regidos por padrões de ordem legal e técnica.

No modelo proposto por Geus (2001 *apud* Pollitt, 1995), existe uma hierarquia a ser respeitada com duas classes: a dos Padrões Legais e a dos Padrões Técnicos. Para cada uma destas classes há também uma hierarquia a ser seguida. A classe dos Padrões Legais é composta inicialmente pelos Princípios Legais e posteriormente pelas Exigências Legais. Na Classe dos Padrões Técnicos primeiramente são considerados os Princípios Técnicos sucedidos pelas Políticas de Análise e posteriormente as Técnicas e Soluções.

Uma abordagem sistêmica para efetuar uma investigação é uma forma interessante, pois apresenta os padrões, que devem conduzir a investigação dos crimes eletrônicos e fraudes computacionais, desde a notificação do incidente até a conclusão do inquérito policial.

Para a padronização adequada, Geus (2001) observa um complicador importante que é quantidade de variáveis intervenientes envolvidas tais como a variedade de exames a serem realizados e a diversidade de tecnologias, que evoluem constantemente. Enfim, é inconteste a necessidade de se manter a criminalística atualizada em relação aos avanços técnico-científicos, e para a consecução desse objetivo a "menina dos olhos" é a forense computacional. Cabe observar, que por um lado a forense computacional é uma disciplina recente e, por outro está ocorrendo uma constante e crescente evolução na utilização de computadores para executar atividades ilícitas. Outro fator que necessita ser considerado com profundidade é o fato das instituições brasileiras não darem apoio para a pesquisa aplicada a esta área.

Deve-se observar que no Brasil as leis vigentes e os recursos disponíveis são diferentes dos adotados pelos americanos. Este é um fato, que exige adaptações e também envolve o interesse em investir nas pesquisas desta área. Para justificar tais investimentos proponho a execução de pesquisas com os objetivos de determinar as áreas das empresas que predominantemente têm sido alvo de fraudes e os prejuízos financeiros decorrentes destas fraudes tais como as indenizações pagas aos seus clientes, as interrupções no funcionamento dos seus serviços além de estimar os valores intangíveis perdidos na maculação da imagem provocada por esses crimes.

3. O TRABALHO COM AS EVIDÊNCIAS: RECONHECIMENTO E IDENTIFICAÇÃO DA CENA DO CRIME

São necessários diversos padrões para especificar as etapas a serem cumpridas no tratamento das evidências na Análise Forense Computacional. As condutas fundamentais a serem seguidas passam obrigatoriamente pelo reconhecimento e identificação das evidências, pela documentação da cena do crime, pela coleção e preservação da evidência e pelo empacotamento e transporte da evidência. E é sobre a abordagem de reconhecimento, a identificação de documentação da cena do crime que é focada a relevância do fator histórico da cena do crime e os benefícios deste para o esclarecimento das evidências.

Nas cenas dos crimes encontra-se uma variedade de dispositivos eletrônicos que devem ser considerados e avaliados. Cada evidência necessita de caracterização posicional e funcional, que serão alvo da investigação. É necessário relacionar os usuários que têm acesso à cena, ou seja, aqueles que poderiam deixar vestígios do crime. Esta atividade recebe a denominação de Configuração do Cenário de Evidências.

Um perito (NIJ GUIDE, 2001) deve identificar as evidências em potencial, relativas ao ambiente e referente aos recursos eletrônicos. Os principais planos a serem seguidos para a avaliação da cena do crime, incluindo os pertencentes à etapa de Reconhecimento são os seguintes:

- Assegurar-se, que todas as pessoas foram retiradas da área em que a evidência será colhida. Neste momento da investigação não se devem alterar as condições de qualquer dispositivo eletrônico. Se um dispositivo estiver desligado, deverá permanecer desligado e, se estiver ligado deixá-lo ligado.

- Proteger os periféricos que armazenam os dados físicos e os eletrônicos. Podem ser encontrados *pagers*, agendas eletrônicas, telefones celulares, e outros dispositivos similares. O Perito

deve sempre estar atento para o fato de que em todo o dispositivo contêm dados e que estes devem ser imediatamente preservados, relacionados e fotografados.

- Identificar e documentar as linhas telefônicas conectadas aos dispositivos, como por exemplo, a linha que atende ao modem e seus dispositivos.

Toda análise de cena de um crime é única e o julgamento das primeiras informações ali contidas pelo investigador devem ser também tratadas como únicas.

O levantamento do histórico pode ser feito através de: entrevistas preliminares, entrevistas com testemunhas e processo de documentação (observação, identificação e registro do local que pode ser feito através de fotografias). Existem peritos que se especializam em abordagens e questionamentos com testemunhas.

Os procedimentos iniciais de Documentação da Cena Física do Crime seguem a seguinte padronização:

- Observar e documentar a cena fisicamente, como a posição do mouse e a localização de componentes;
- Documentar as condições e localização do sistema de computador, incluindo o status de energia do computador (ligado, desligado, em modo de espera, ou se está hibernando). Muitos computadores têm luz de status que identificam se estão ligados. Igualmente, se o *cooler* faz barulho é uma indicação que ligado. Se o computador está com sua temperatura alta pode também indicar que ele está ligado ou que foi recentemente desligado.
- Identificar e documentar componentes eletrônicos que não serão coletados ou enviados para uma análise minuciosa em local apropriado (laboratório forense);
- Fotografar e registrar a cena para criar uma gravação visual e quando possível fotografá-la em 360º.
- Fotografar a frente do computador bem como o monitor, sua tela e outros componentes. Coletar anotações em que apareçam no monitor do computador. Programas em execução na tela podem precisar de gravações em vídeo ou descrição de sua atividade no monitor.

A Documentação da cena é importante (NIJ GUIDE, 2001), pois cria uma permanente gravação do histórico da mesma e assegura a precisa localização e condições dos computadores, mídias de armazenagem, outros dispositivos eletrônicos e evidências convencionais, ou seja, a base da investigação é feita neste momento.

Muitas vezes testemunhas podem ser solicitadas para esclarecer aspectos durante o processo de investigação e também em qualquer ponto de limitação deste, ou seja, auxiliam os peritos a esclarecer fatos das evidências examinadas, dando direções por ele não percebidas. Esta é a importância de se obter e manter o histórico do acontecimento para poder direcionar a investigação, a própria coleta de evidências e posteriormente em outra fase de classificá-las.

Assim como os procedimentos para Documentar a Cena do Crime, seguem exemplos de condutas para entrevistas preliminares:

- Separar e identificar todas as pessoas (observadores e pessoas presentes, suspeitos ou demais pessoas encontradas) na cena e gravar suas localizações;
- De acordo com o departamento de polícia e leis aplicáveis tanto no Brasil como em outros países, obter destas pessoas individualmente informações pertinentes ao incidente.

São informações pertinentes ao incidente, que auxiliam o processo:

- Proprietários e usuários dos dispositivos eletrônicos encontrados na cena, bem como as senhas, nomes dos usuários e serviços de provedores;
- Senhas. Qualquer senha requerida para acessar o sistema, software ou dados. (senhas de BIOS, *logins* de sistemas, rede ou ISP (Internet Service Provider), arquivos de aplicação, demais acessos e ou listas de contato);
- Funcionalidade do sistema;
- Qualquer esquema de segurança único ou dispositivo de destruição;
- Qualquer armazenamento de dados externo;
- Qualquer documentação do *hardware* e *software* instalado no sistema.

4. CONCLUSÃO

Com este trabalho pode-se concluir, que ao pesquisar sobre o histórico do início dos trabalhos em estabelecer normas nesta área, é possível notar como estas empresas, instituições e organizações se reuniram.

Aparentemente possuíam objetivos e iniciativas em comuns, levantaram e identificaram as necessidades e deram início as variedades de classificações conhecidas hoje pela Forense Computacional. Foram especializando em cada assunto e aprofundando os conhecimentos nas suas linhas de conduta. Contribuíram para gerar as informações que puderam ser disponibilizadas e difundidas.

O trabalho teve fundamentação na pesquisa científica e ganhou cada vez mais contribuições sobre o assunto. É interessante ver como eles se organizaram e permitiram trabalhar para unir esforços montando os vários tipos de órgãos encontrados.

Há benefícios em se usar guias sistêmicos e se criar metodologias não somente para o levantamento do histórico de evidências nas cenas de crimes eletrônicos como exposto e descrito neste trabalho, mas para todas as outras áreas e atividades que cercam esta ciência. Tendo em mãos procedimentos claros e passos a seguir o trabalho do perito se torna ágil e eficaz.

Vale lembrar todos os cuidados que estes guias sugerem e a série de fatores que devem ser lembrados até mesmo notificados e seguidos durante as investigações. Estes guias também ressaltam a importância de seguí-los com vigor.

Devem sofrer por atualizações à medida que aparecerem novos tipos de crimes, ou seja, novas formas de ataques relatados, mas sigam aos modelos e padrões aceitos e revisados.

Muito importante também é promover fóruns, seminários para discussão e treinamentos assegurando a disseminação de conhecimentos e principalmente as qualificações de investigadores pelas infrações na esfera computacional.

5. REFERÊNCIAS BIBLIOGRÁFICAS

SEBADASH, Victor. *Criminal Legal Description of Computer Crimes: Methods and Practice of Investigation.* On-line. 09 de Jun. 2004.Disponível em <http://www.crime-research.org/articles/Sabadash0504/>. Acesso em 01/06/2004.

GOLUBEV, Vladimir. *Computer Crime Classification.* On-line. 04 de Mai. 2004. Disponível em <http://www.crime-research.org/articles/Golubev0504/>. Acesso em 10/06/2004.

CHAWKI. Judge Mohamed. *The Digital Evidence in the Information Era.* On-line. 10 de Mar. 2004. Disponível em http://www.crime-research.org/articles/chawki1/. Acesso em 15/06/2004.

POLLITT, M. *Computer Evidence Examinations at the FBI*. Unpublished presentation at the 2nd International Law Enforcement Conference on Computer Evidence, Baltimore, Maryland, April 10, 1995.

GOMEZ, Leopoldo Sebastián M.*Marco Normativo de Perícias em Infomática.* On-line. Disponível em <http://www.e-evidence.info/international.html> Link: Argentina. Acesso em 01/06/2004.

SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE. *SWGDE Recommended Guidelines for Validation Testing.* .USA, Orlando, Flórida, 2004. Versão-1. Disponível em <http://ncfs.org/swgde/documents/swgde2004/>. Acesso em 10/06/2004.

NIJ GUIDE - U.S. DEPARTAMENT OF JUSTICE - NATIONAL INSTITUTE OF JUSTICE. *Electronic Crime Scene Investigation: A Guide for First Responders.* On-line. Jul 2001. Disponível em <http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm>. Acesso em 05/06/2004.

GEUS, Paulo Lício de. *Forense Computacional Procedimentos e Padrões*. In: SIMPÓSIO DE SEGURANÇA EM INFORMÁTICA – ITA, 24/10/2001. Disponível em <http://linorg.cirp.usp.br/SSI2001/artigos.html>. Acesso em 01/06/2004.

UNITED STATES DEPARTAMENT OF JUSTICE. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. USA, 2002.

FORENSIC COMPUTER CRIME INVESTIGATION. ***Electronic Forensics in an International Environment***. London and Manchester, UK, 2004

SISBRAV
SISTEMA BRASILEIRO DE ALERTA DE VULNERABILIDADES
(BRAZILIAN VULNERABILITY ALERT SYSTEM)

Daniel Silva Almendra[1], Leonardo Lobo Pulcineli[1],

Robson de Oliveira Albuquerque[2], Rafael T. de Sousa Jr[3].

Universidade de Brasília
Campus Universitário Darcy Ribeiro
Faculdade de Tecnologia
Departamento de Engenharia Elétrica e Redes de Comunicação
Brasília – DF – Brazil
[1]{danielalmendra, pulcineli}@terra.com.br
[2]{robson}@redes.unb.br
[3]{desousa}@unb.br

Abstract

This paper describes the project and implementation of a vulnerability search and alert system based on free software. SisBrAV (acronym in Portuguese for Brazilian Vulnerability Alert System), will consist in a spider mechanism that explores several security-related sites for information on vulnerabilities and an intelligent interpreter responsible for analyzing and sorting the relevant data, feeding it into a database. With that information in hands, an email notifier sends out alerts, in Portuguese, about new vulnerabilities to registered clients, according to the operating systems and services run in their environment. In addition to the email notifier, a web server will also be implemented, for systems administrators to perform an on-demand custom search in the vulnerabilities database.

1. INTRODUCTION

In a daily basis, a large number of vulnerabilities, which affect a variety of systems and services, are detected. Manufacturers and developers work extensively in order to release, as fast as possible, a patch that fixes the problems found in their products. On the other hand, the hacker community is continually growing, producing malicious codes, exploits and viruses that take advantage of those vulnerabilities very rapidly. With the incredibly large quantity of information that can be found on the Internet today, as well as the increasing number of hacker sites that provide easy access to lots of malicious tools and exploit codes, it is of great importance that every enterprise's systems security team be well advised and informed about what are the threats to their environment and what they can do to avoid them, protecting their systems, services and network quickly and proactively. Even individuals with one or two PCs at home should be concerned with their system's vulnerabilities, applying the latest patches in their software, avoiding any security problem that may happen.

Existing vulnerability database systems are created and maintained by human administrators, who are responsible for searching, analyzing and evaluating new vulnerabilities everyday, and then updating the database regularly with new entries, in a pretty much manual process. The initial idea of the project depicted in this paper, was that there could be an automatic process of gathering the relevant vulnerabilities information, sorting it according to predefined rules, feeding a database and generating email alerts for specific recipients whose environment could be affected. The solution should be based on free software and should also be portable to many platforms. SisBrAV project is, thus, the result of that idea.

2. RELATED ISSUES

Up to this date, in Brazil, there isn't any system such as SisBrAV, which automatically looks for new vulnerabilities and informs the users about them. In the other hand, a large number of security sites can be found in the Internet, and almost all of them have a vulnerability alert section, updated daily, enclosing vulnerabilities for many systems and programs. Thus, information regarding vulnerabilities can be easily accessed through the Internet, but it is very difficult to glimpse which vulnerabilities represent real threats among the large number encountered. So, there is plenty of information, but a lack of simplicity in the process of filtering these pieces of information, in order to keep only in the important ones.

The main challenge in the SisBrAV project is the sorting process, since the system will search for vulnerabilities in many sources, and each of them organizes the information in a particular way. The interpretation of the data collected must be very precise, as well as the sorting process, since the clients must be informed only about the threats to his specific environment. The importance score for each vulnerability must also be precisely assigned, making it possible for the client to assign different priorities when establishing security countermeasures for the vulnerabilities he has been informed about.

Two other elements are also critical for the efficiency of the SisBrAV system: the organization of the vulnerability information and the generation of customized alerts to each client according to his systems and services. The information must be sorted in an accurate but simple manner, and the alerts must be clear and succinct, as well as they must be sent only to the clients whose environment is threatened by the vulnerabilities.

SisBrAV will implement a module for each function it performs. The following section will describe how all these modules work and what functions they perform.

3. SISBRAV MODULES

SisBrAV will be consisted of 5 modules. The Vulnerability Search Mechanism (VSM) module will consist in a spider that accesses and indexes many vulnerability documents in several security sites. The Interpreter, Parser and Sorter (IPS) module will be a program that analyses the data provided from the spider, defining priorities and classifying the entries, according to predefined rules. The Central Database (CDB) module will store all vulnerability data, clients' info and keywords for English-Portuguese translation. The Email Notifier (E-Note) module will alert by email the registered clients about new/updated vulnerabilities specific to each client's environment. At last, the Vulnerability Web Server (VWS) module will be a server, accessible by any registered client, to perform an on-demand, customized vulnerability search in the Vulnerability Database. The details of each module are depicted in the next sections.

3.1. Vulnerability Search Mechanism (VSM)

The vulnerability search and indexing process is made by a spider mechanism. A spider is a program that explores the Internet by retrieving a document and recursively retrieving some or all the documents that are referenced in it. It acts as an untiring human being who follows all links he finds in a web site, and all the links in the subsequent documents he sees. The spider indexes (fully or partially) all the documents that it accesses into a database, which can afterwards be used by a search engine.

The spider tool used in SisBrAV will be *htdig*, which is one of the programs that constitute the *Ht://Dig* package (6). *Ht://Dig* is a free web search engine, created in accordance to the GPU (General Public License) rules, and is consisted of many individual programs, like *htdig*, *htdump* and others.

The most recent stable version of *Ht://Dig* is 3.1.6, so this will probably be the version implemented in SisBrAV. A brief description of the *htdig* program is necessary, for there are some options that are used in the system, for its best performance and accuracy.

Htdig is a spider program (or search robot), which does what is called the "digging" process, retrieving HTML documents using the HTTP protocol, gathering information from these documents

and indexing them, creating specific database files which can then be used to perform a search through these documents.

Htdig has many options, which are/will be used in the SisBrAV system, either to produce a desired result or for debugging purposes. The *–c <configfile>* option specifies another configuration file instead of the default. Another important option is the *-h <maxhops>* option, used to restrict the dig to documents that are at most maxhops links away from the starting document. This option is used every time the initial digging is run, to assure that htdig will index only the relevant documents for each site. The *–i* option is used to perform an initial digging. With this option, the old databases are removed, and new ones are created. There are also some options very useful for debugging, such as *–s* and *–v*, used to print statistics about the dig after completion and to set the verbose mode, respectively. For test purposes, one important option is the *-t* option, which tells *htdig* to create an ASCII version of the document database, making it easier to parse with other programs, so that information can be extracted from it for purposes other than searching. It generates the files *db.docs* and *db.worddump*, which formats will be explained later. Finally, the *url_file* argument can also be passed, telling *htdig* to get the URLs to start indexing from the file provided, overriding the default *start_url* in the configuration file.

As said before, when using *htdig* with the *–t* option, it produces two ASCII files, *db.docs* and *db.worddump*. The *db.docs* file contains a series of lines, each of them relating to an indexed document. The lines contain information such as the document URL, title, modification time, size, meta description, excerpt, and many other useful document information. The *db.wordlist* file has a line for each word found in the indexed documents. Each line in this file contains a word, followed by the document ID where it was found, its location in the document, its weight, number of occurrences, etc.

The default configuration file for *htdig* is the file *htdig.conf*. That's where all configuration options for *htdig* (and the other tools, if they are used) are set. Since all of its parameters will probably be left with their default values, this file's content will not be copied in this paper. At first, the security sites indexed by SisBrAV's *htdig* will be the ones listed in the items (5), (7), (8), (9) and (10) in the References section. The number of sites can be (and will be) expanded to a much higher number, but initially only these five sites were chosen. The way *htdig* indexes each site will be almost the same: the only parameter that will differ from one site to another is the number of hops from the starting URL. For example, if *maxhops* is set to 2, *htdig* will index the starting URL, then it will follow all the links in that URL and index all the documents, and finally it will also follow the links in these documents, indexing the documents it finds, and then stop the digging process. Since each site has its way of displaying their documents, the number of hops necessary to gather all relevant vulnerability information will vary from site to site.

To solve this issue, a simple UNIX bash script will be used to read a file that contains lines with an URL and a number (which defines the maximum hops from the initial URL), separated by a TAB. The script will produce different *htdig* commands, according to the number of maximum hops defined. The number of maximum hops for each site is defined by the SisBrAV administrators, who inspect the sites and check the number of levels the spider will have to crawl down in order to obtain the maximum amount of relevant information about the vulnerabilities, and the minimum unnecessary information.

Htdig generates several Berkeley DB type files. These files will then be analyzed by the IPS Module, as explained in the next section.

3.2. Interpreter, Parser and Sorter (IPS)

The IPS Module will probably be written in Java. It will use an heuristics algorithm to perform the content analysis of the data stored in the Berkeley DB files created by *htdig*, in order to feed the Central Database with accurate vulnerability information. The data is parsed and the vulnerabilities are grouped between previously determined, hierarchically distributed classes.

At first, the IPS program will perform the sorting process. Initially, it analyses all the entries in the database, to find ambiguous or duplicated information for a same vulnerability. Then, it parses the content of the information, in order to group the vulnerability entries in classes, according to its main aspects: remote/local, type, low/medium/high importance score, etc. It also determines the systems/services in which that vulnerability occurs. If there is more than one entry for the same

vulnerability, it correlates all the information found in the entries, to make sure the attributes are set as precisely as possible. For example, if a given vulnerability is issued in three different sites, and one of them scores the vulnerability as of medium importance and the others say its importance is high, the IPS will set this attribute to "high".

The hierarchical class tree used to group the vulnerabilities is described in Fig. 1.

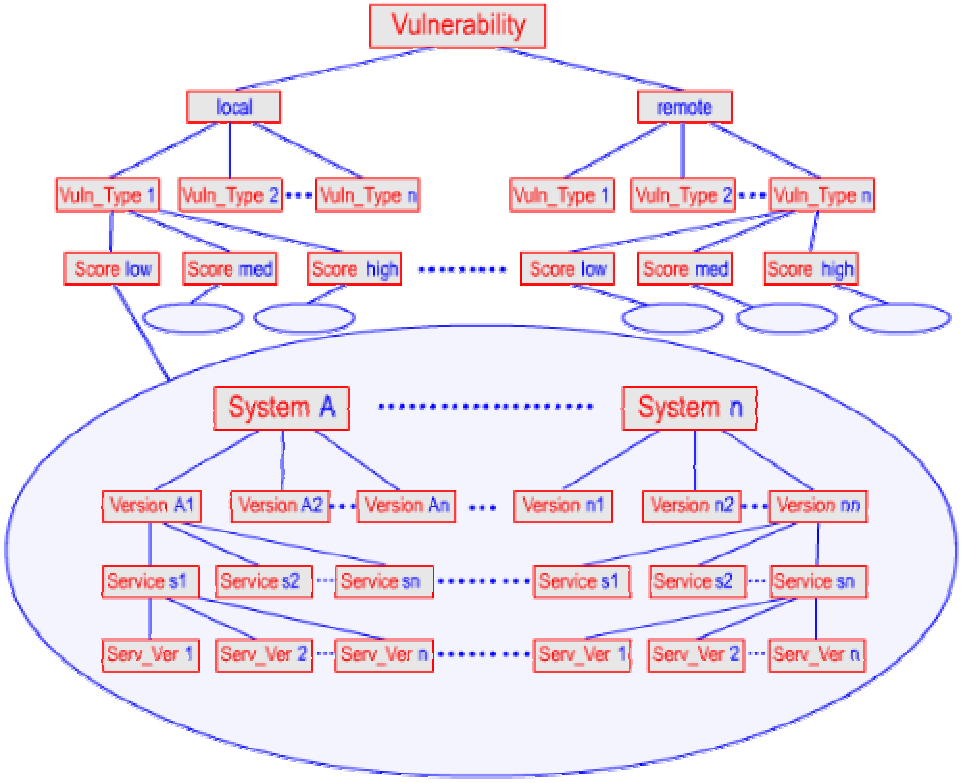


Fig. 2. IPS – Hierarchical Classes Tree: the vulnerabilities are sorted and grouped into different classes

Each document indexed by the spider in the VSM module will be related to a specific vulnerability. The IPS module performs the vulnerability sorting process for each document, by following the tree shown in the above figure. Initially, the algorithm determines if the vulnerability is local or remote, according to the information found in the document. It then classifies the vulnerability into a specific vulnerability type, among the predefined types registered in the system, such as Denial of Service, Buffer Overflow, Password Retrieval, Authentication Bypass, etc. Afterwards, an importance score is assigned to the vulnerability. At last, the IPS finds out what operating systems – and their versions – are affected by the vulnerability, and what programs/services – and their versions – are threatened by it. As well as the vulnerability types, there will also be a large list of systems and services (and their respective versions), which IPS will use in the sorting process.

After a given vulnerability is sorted, the IPS checks if there is any other vulnerability with exactly the same characteristics, affecting the same systems/services. If so, it performs a series of tests, to check if both entries refer to the same vulnerabilities. In these tests, other information is analyzed, such as the vulnerability date, the document URL (if the root site is the same, it's probably not the same vulnerability, since a security site must not have duplicated documents for the same vulnerability), and other information.

After the vulnerabilities have been classified, the IPS feeds the Central Database with that data. Since the database is not hierarchical, but relational, the IPS will also have to convert the results of the sorting process before actually feeding the Central Database.

3.3. Central Database (CDB)

In order to store all the information regarding vulnerabilities and their attributes, clients' profiles, systems and services data, as well as the English-Portuguese translation data, SisBrAV will have a Central Database. It is most likely that it will be implemented using a MySQL server, which is GPU compliant, and its architecture will follow the SQL ANSI standard, to guarantee its portability and scalability.

The CDB will be divided into three smaller databases, each one storing specific information, although the three of them relate to each other. The first database is the Vulnerability Database, which will contain all the vulnerability information already sorted into defined groups, as seen in the IPS section. The second base is the Client Database, which will keep the client-related data, such as their names, contact information and the systems and software running in their environment. At last, the third database will be the English-Portuguese Translation Database, storing a number of keywords, each one relating to keywords in the other idiom, according to certain parameters.

Mostly based on the schema designed by the Open Source Vulnerability Database Team (5), the Vulnerability Database is the most important part of the whole SisBrAV system, for it is the central repository of all vulnerability information. Its structure, which is still being developed, will probably keep the main OSVDB structure, although there will be some changes in certain tables, and other tables will be removed or added. The Vulnerability Database, when fully implemented, will be similar to Fig. 2.

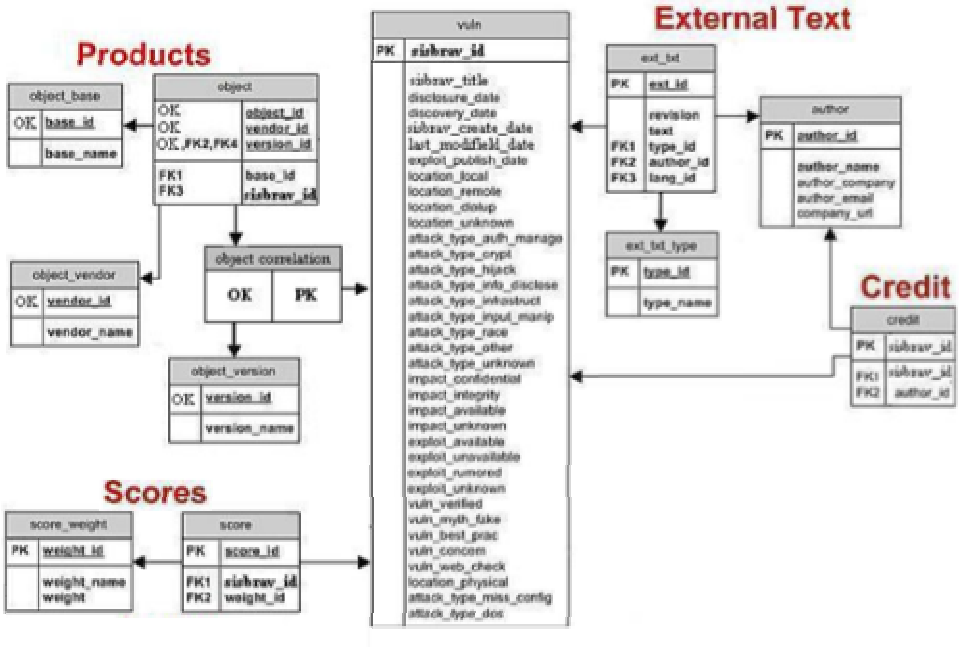


Fig. 3. Vulnerability Database schema

The External Text section in this database consists in tables that describe certain aspects about a vulnerability. They exist inside the database, but usually describe information that one would use externally to the database. For example, a Solution Description, or a Vulnerability Description is an external text.

The tables in the above schema also deserve some explanation. The *vuln* table is the main table in the schema. It's where the SisBrAV IDs live. Other information stored in this table includes various dates and vulnerability classification data. The *ext_txt_type* table defines the types of external texts. For example, Vulnerability Description, Solution Description, Technical Description, Manual Testing Notes. The *ext_txt* table stores the external text blobs for any type of text that is larger than 1024 characters. Other information stored is the language, type, author, and revision. When the texts are updated/fixed/modified the new text is reinserted into this table and the revision number is

incremented. The contributors for anything in the *ext_txt* table are identified in the *author* table, making it possible to have a contributor's line to any SisBrAV ID. The authors are used to track the external text authors, as well as the credited researcher of each vulnerability. In the Products section, the *object correlation* table performs a link between the PK of the vuln table and a key named Object Key (OK). As a result, it is possible for other tables to link to the Products tables without using a PK. The *object* table binds vendor, base, version and vulnerability together, storing product information. The name object might seem sort of vague, but it means the object that the vulnerability exists within. The *object_base* table contains product names. For example, Windows, Exchange, Apache, and MySQL are all examples of product names. The *object_vendor* table contains the vendor names. For example, Microsoft, Sun Microsystems, and Apache Software Foundation are all examples of vendor names. The *object_version* table contains the version names. For example, 1.0, 2.0, 0.1, XP, 2000, or 95 are all examples of version names. Another crucial table is the *score* table, used to bind a scoring weight to a vulnerability. It is intended to allow every vulnerability in the database to be associated with one scoring weight. The *score_weight* table is used to store any type of scoring information needed for scoring calculations. Finally, the *credit* table adds support for identifying credit for discovering a vulnerability. Instead of storing author like information, a reference to the author table is made, as the data is extremely similar.

The second part of the CDB is the Client Database, responsible for storing all client-related data, involving personal/enterprise identification information, contact emails, products (systems and services) running, etc. Its structure is shown in Fig. 3.

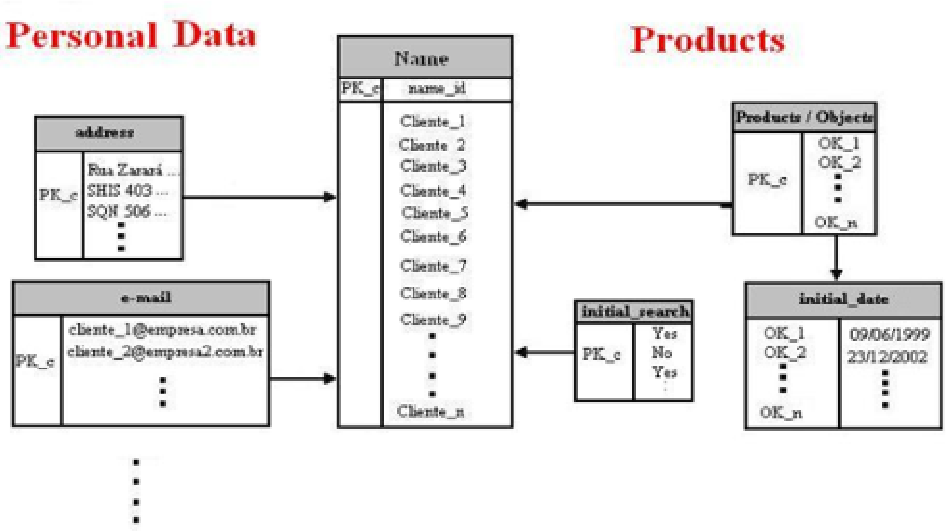


Fig. 4. Client Database schema

In the above schema, the Products section refers to the products that each client registers, in order to receive only vulnerability alerts related to the systems running in his/her environment. The initial date to look in for vulnerabilities is also stored for each client. Specific product characteristics data is kept in the Vulnerability Database, as it was shown in the previously. All data related to a client himself is found in the Personal Data section. Contact emails, telephone numbers, addresses and personal/enterprise information, as well as the clients' passwords are entered in this part of the database.

The *Name* table consists in the main table of the Client Database, containing each client's account ID. All the clients are bound to their products through the *Products/Objects* table. The *initial_date* table stores the initial date to search for vulnerabilities, for each product a client registers in the database, while the *Initial_search* table contains entries that specify if a client is a new registered client in the system (represented by a "Yes" entry) or not ("No"). These entries are used by E-Note, to define if an initial search must be executed or not. At last, the Personal Data tables, such as

address, *e-mail* and others, store client specific information, such as email, telephone numbers, address, personal/enterprise information and login username and password.

The last subpart of the CDB is the English-Portuguese Translation Database, which is still being designed. It will contain a large number of keywords in English and in Portuguese, in addition to semantics and syntax rules, making it possible for the E-Note module to translate the main description of a vulnerability entry to compose a mainly Portuguese email alert.

3.4. Email Notifier (E-Note)

This program will look for updated vulnerability information in the database. After retrieving the information, the program checks, for each registered client, if there are any new/updated vulnerabilities which affect the client's environment. If so, an email message – in Portuguese – is formatted, to inform the client about the new vulnerabilities discovered in his systems and services. This message consists in a brief explanation of the vulnerability, in Portuguese, and one or more links for further information on that issue.

When a client registers in the SisBrAV system, he will have to inform what systems he has and what programs he runs, thus defining the scope of vulnerabilities SisBrAV should be concerned with, when generating alerts to that specific client. Besides that, the client also defines the start date, determining the initial point from which the system should begin the search in the vulnerability database. With that data in hands, E-Note will search in the database only the information that is really necessary for that client, generating a customized email message to him.

The E-Note module will also be written in Java, to guarantee its portability. E-Note is divided in two programs: one program performs the search in the database and the other sends the email alert.

For each new client added in the system, all the data about his systems and services is stored in the clients table, in the SisBrAV database, and a flag is set for this client, with a logical value that represents "NEW". The start date from which he wants to be informed about existing vulnerabilities is also stored in the database clients table.

Every time E-Note is run, it checks if there are any new clients in order to search for all the vulnerability entries that occur specifically in their systems and are newer than the start date defined by the client. It then generates the email alert to those clients, notifying about all vulnerabilities found. Afterwards, the "NEW" flag in the clients' entry in the database is set to a value that stands for "OLD".

For existing clients, the E-Note will simply check if there are new/updated vulnerabilities regarding their systems/services. If so, it generates the email alert for the specific clients whose systems are affected.

Due to the fact that the vulnerability information stored in the database is mainly in English, the vulnerabilities selected by E-Note are also in English. To make it possible for E-Note to generate Portuguese messages, an English-Portuguese translation database will bind English keywords to previously defined Portuguese sentences. E-Note performs, thus, a simple translation in the main vulnerability description. The main aspects – remote/local, high/low importance, etc – of the vulnerability are also translated. For example, if the main description of a vulnerability is "HP-UX DCE Remote Denial of Service Vulnerability", and its importance is critical, the Portuguese message would be "HP-UX DCE: Vulnerabilidade Remota de Negação de Serviço. Importância: Crítica". The translation database is in the format described in the previous section.

Along with the main description of the vulnerability, the email also contains links to the sites where that vulnerability is described and discussed.

3.5. Vulnerability Web Server (VWS)

The idea of SisBrAV is not only to inform its users, emailing them alerts about vulnerability issues. The registered clients will also be able to perform a custom search in the Vulnerability Database through the web. With that functionality in mind, the fifth module of SisBrAV will be a Web Server that will handle these web requests.

The users will access an authentication site, where they provide their username and password (which are created and informed to him/her during the registering process). If successfully authenticated, they will be redirected to a customized database search page.

The site interface is being designed to be friendly and simple, although its security will be fundamental. The web site will probably be based in PHP, due to the fact that this language is very portable, and through its use, the database access can be implemented in a secure and simple manner. The web server chosen for the SisBrAV system was Apache, mainly because it is a multi-platform server, and also because fully supports the web publishing technology which will probably be used (PHP).

There are also other technologies which utilization is currently in discussion, such as Java servlets or JSP, because through using it would be easier to integrate the VWS module to the other modules in SisBrAV. XML is also in discussion, since it is another efficient way of implementing the database access from web. If JSP ends up being implemented, Tomcat (which is the servlet container that is used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies, fully integrated with Apache) will also be used.

4. CONCLUSIONS

In the current scenario, it is really important for anyone connected to the World Wide Web to protect his/her systems and data against the threats that continually arise. Besides having a nice antivirus tool, a firewall efficiently configured and other security technologies implemented in their network, users and enterprises must keep all of their Operating Systems, services and other software up-to-date, by applying all their latest patches and fixes. With that in mind, it's of great importance that systems and network administrators be informed quickly about any vulnerability that may be encountered in their systems, so that they can act proactively to build up defense countermeasures to guarantee the security of their environment.

SisBrAV will be an important security innovation, since it implements an idea of an automatic vulnerability searching and alerting mechanism, with very little human administration needed. Since it will have many trustable security sites as sources where it will look for vulnerabilities information, SisBrAV will be a very reliable system, extending the horizons of systems and network security. In addition to that features, it is also important to remember SisBrAV, being a Brazilian project, will implement a translation feature in order to produce Portuguese email alerts, so that Brazilian clients will feel comfortable with it. In the future, the language support can be expanded to other idioms.

Nowadays, where free software gradually gains space in the software business, a program must support many platforms, so that it can be installed in a variety of systems and interact with different technologies without incurring into stability loss or performance troubles. SisBrAV is being designed using only free software products and platform independent languages, resulting in a solution with great portability and scalability.

5. REFERENCES

1. Deitel, H. M. – Java, Como Programar / H. M. Deitel e P. J. Deitel; trad. Carlos Arthur. Lang Lisboa. – 4.ed. – Porto Alegre: Bookman, 2003.
2. SQL Tutorial. Available from: http://www.w3schools.com/sql.
3. PHP/MySQL Tutorial. Available from: http://www.freewebmasterhelp.com/tutorials/phpmysql.
4. Portal Java Home Page. Available from: http://www.portaljava.com/home/index.php.
5. Open Source Vulnerability Database. Available from: http://www.osvdb.org.
6. Ht://Dig Project Home Page. Available from: http://www.htdig.org.
7. Internet Security Systems X-force Home Page. Available from: http://xforce.iss.net.
8. Cert Knowledge Base. Available from: http://www.cert.org/kb.
9. SANS Newsletters. Available from: http://www.sans.org/newsletters.
10. Security Focus Home Page. Available from: http://www.securityfocus.com.

INFORMÁTICA FORENSE: FORMATO DE IMAGENS FOTOGRÁFICAS DIGITAIS E SEUS REFLEXOS NA ANÁLISE PERICIAL

Rafael Pinto Costa, Sérgio Luís Fava

Serviço de Perícias em Informática – Instituto Nacional de Criminalística
Polícia Federal – Brasília – DF

Emails:rafael.rpc@dpf.gov.br, fava.slf@dpf.gov.br

Abstract

This paper describes the forensics examinations conducted on a computer probably used to commit crimes against children. The computer´s owner was a likely suspect of child molestation, supposedly convincing them to follow him to his house, having sex and taking pictures of them. The concepts about graphic file formats for digital imaging are explained. A topic about how data is organized on hard disks is also included. All the processing steps taken by the computer experts are shown in details.

1. INTRODUÇÃO

O combate à exploração sexual de crianças e adolescentes constitui um tema que atrai atenção constante. Diversas iniciativas de investigação e repressão a esta atividade têm sido desencadeadas atualmente, como por exemplo, a Comissão Parlamentar Mista de Inquérito (CPMI) criada pelo Congresso Nacional e cujos trabalhos se estenderam de junho de 2003 a junho de 2004 [CPM 04].

Por se tratar de um tema com forte apelo emocional, a exploração de imagens contendo cenas de sexo envolvendo crianças e adolescentes causa repúdio generalizado da sociedade, principalmente devido à facilidade de divulgação através de meios como a Internet. Neste sentido é importante destacar a existência de dois agentes distintos: aquele que coleta e divulga material pornográfico infantil pela Internet e aquele que produz o material. Este último merece atenção especial das autoridades dada a gravidade de suas ações e porque atua como fonte para atuação dos demais.

Uma ferramentas bastante utilizada atualmente na produção deste tipo de material é a máquina fotográfica digital. Os dois principais motivos para isto são a baixa exposição dos responsáveis (uma vez que não é necessário utilizar um laboratório de revelação comercial) e a facilidade de manipulação das imagens geradas, proporcionando a ocultação de detalhes que poderiam levar à identificação dos criminosos.

Este artigo apresenta um caso real de perícia envolvendo o computador de uso pessoal de um suspeito de produção de material pornográfico infantil. Neste caso em particular, o material examinado não apresentava indícios de publicação do material na Internet, nem mesmo a remessa para outras pessoas, assumindo proporções de um crime "local", mas não menos grave.

A exposição que segue está restrita aos aspectos técnicos utilizados durante os exames, esclarecendo o método utilizado para recuperação e seleção da grande quantidade de material encontrada. As seções 2 e 3 apresentam detalhes sobre os principais formatos de armazenamento utilizados em fotografias digitais, enquanto que a seção 4 procura esclarecer alguns aspectos fundamentais sobre a organização de arquivos em computadores. A seção 5 demonstra a aplicação

destes conhecimentos técnicos em um caso real de exame e, por fim, a seção 6 lista as considerações finais a respeito do tema.

2. MÁQUINAS FOTOGRÁFICAS DIGITAIS – ARMAZENAMENTO DE IMAGENS

Sem considerar o tipo de mídia utilizado, as máquinas digitais disponíveis atualmente armazenam as imagens capturadas em arquivos estruturados em um dos três formatos principais:

- **JPEG (*Joint Photographic Expert Group*)** – formato mais utilizado tendo como características básicas a compressão do arquivo e o conseqüente armazenamento da imagem com perda de qualidade [JPG 04][1]. Apesar disso, dependendo do nível de compactação utilizado a perda na qualidade da imagem não é perceptível ao olho humano. É o formato mais adequado, por exemplo, para imagens publicadas via Internet e satisfatório para impressão de fotografias [CHA 04].

- **TIFF (*Tagged Image File Format*)** – formato de qualidade superior normalmente utilizado sem compressão e que por esta razão ocupa maior espaço de armazenamento.

- **RAW** – normalmente referenciado como o verdadeiro negativo digital. Com um arquivo de imagem nenhum processamento é efetuado pela câmera sobre a imagem fotografada, permitindo controle total ao fotógrafo. Normalmente disponível apenas em máquinas mais avançadas, não existe um formato padrão definido para este tipo de arquivo, variando de acordo com o fabricante do equipamento. Não utilizado em larga escala e não reconhecido por todos editores de imagens.

3. FORMATO DOS ARQUIVOS JPG E A EXTENSÃO EXIF

Devido a sua praticidade e ao fato de as imagens geradas ocuparem menor espaço nas mídias de armazenamento (Compact Flash, Memory Stick, etc.), o formato JPG é o mais difundido na fotografia digital. A grande maioria das câmeras digitais usa na verdade uma variação do formato JPG denominada EXIF.

Este padrão permite a gravação pela câmera de informações adicionais no arquivo de imagem gerado. O padrão EXIF foi desenvolvido pela Associação de Desenvolvimento da Indústria Eletrônica Japonesa (JEIDA) [JEI 02], sendo sua versão atual a de número 2.2.

A informação extra armazenada nos arquivos está relacionada com as condições em que a fotografia foi tirada, os ajustes utilizados na câmera, a codificação de cores, além de diversas outras possibilidades. O que é realmente gravado depende do modelo do equipamento utilizado.

Na figura 01 mostra-se um arquivo de imagem gerado por uma máquina da Sony. Ao lado da imagem são expostas algumas informações adicionais disponíveis no arquivo como: marca e modelo da máquina, data, tempo de exposição, etc.

[1] Do ponto de vista técnico estrito JPG não representa um formato de arquivo, mas sim uma família de algoritmos de compressão de imagens. Algumas empresas desenvolveram formatos proprietários de arquivos enquanto o padrão de fato se tornou aquele identificado como JFIF (JPEG File Interchange Format).

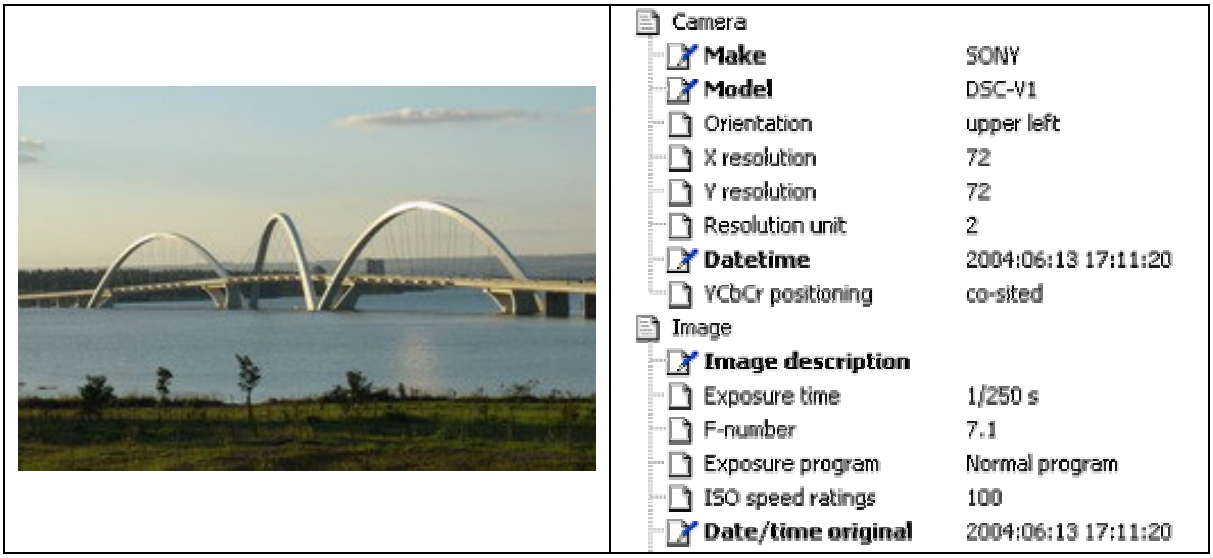


Figura 01: Exemplo de fotografia digital e de informações adicionais presentes no arquivo gerado

3.1. Formato do Arquivo e Marcadores Especiais

Todo arquivo JPG começa com o valor hexadecimal '0xFFD8' e termina com '0xFFD9'. Estes são dois marcadores especiais que significam, respectivamente, início de imagem (SOF - Start of Image) e fim de imagem (EOI - End of Image). Existem muitos outros marcadores em um arquivo JPG, sendo que sua forma geral obedece à estrutura binária descrita abaixo:

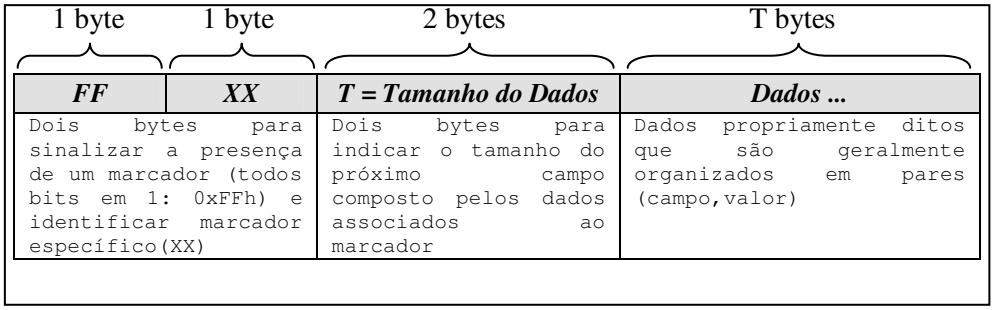


Figura 02: Estrutura geral dos marcadores especiais

O marcador utilizado para armazenar as informações adicionais no formato de arquivo EXIF é um marcador de aplicação identificado pela seqüência 0xFFE1. Todos os dados EXIF são armazenados dentro desta área que está logo no início do arquivo, conforme figura 03.

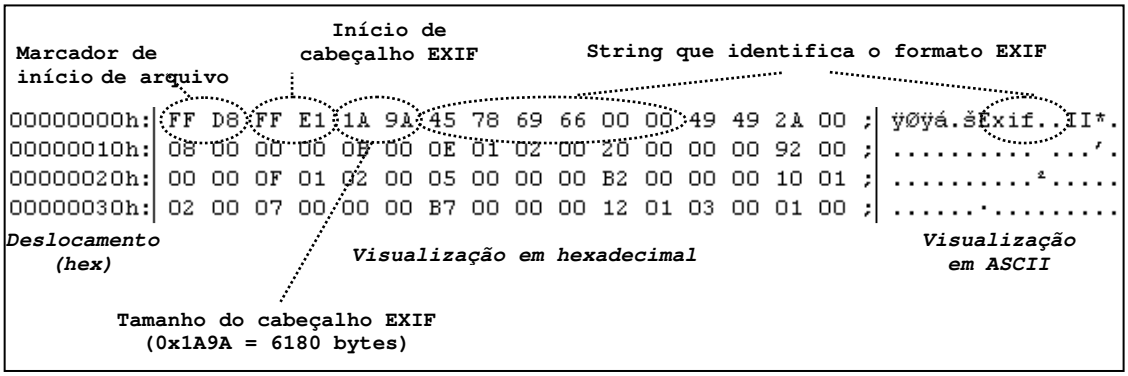


Figura 03: Fragmento da porção inicial de um arquivo de imagem fotográfica digital

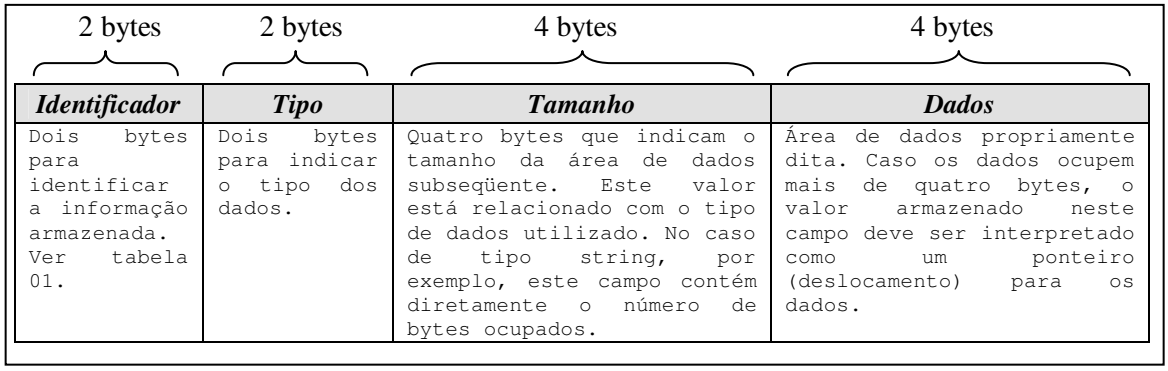
A primeira parte dos dados desta área é uma string especial utilizada justamente para identificar o padrão – os caracteres "EXIF" seguidos de dois bytes nulos.

3.2. Formato do cabeçalho EXIF

Esta área de informações adicionais está organizada em uma lista encadeada de IFDs (*Image File Directory*). Como mais de uma imagem pode ser armazenada em um arquivo JPG, cada IFD está relacionada com uma imagem, agregando uma série de informações a seu respeito.

As câmeras digitais costumam guardar duas entradas nesta área. Uma contendo as informações da imagem principal fotografada (IFD0) e outra contendo informações sobre a miniatura desta mesma imagem (*thumbnail* – IFD1). A miniatura é armazenada no mesmo arquivo JPG e serve para visualização da imagem no visor LCD das câmeras, evitando que toda imagem seja processada e reduzida a cada exibição no visor.

As informações disponíveis em cada IFD são organizadas em registros de 12 bytes, compostas de campos formados por identificadores (tags), tipo, tamanho e dados, conforme estrutura abaixo:



Identificador	***Tipo***	***Tamanho***	***Dados***
Dois bytes para identificar a informação armazenada. Ver tabela 01.	Dois bytes para indicar o tipo dos dados.	Quatro bytes que indicam o tamanho da área de dados subseqüente. Este valor está relacionado com o tipo de dados utilizado. No caso de tipo string, por exemplo, este campo contém diretamente o número de bytes ocupados.	Área de dados propriamente dita. Caso os dados ocupem mais de quatro bytes, o valor armazenado neste campo deve ser interpretado como um ponteiro (deslocamento) para os dados.

Figura 04: Formato geral dos registros de informações

Identificador	***Significado***	***Tipo dos dados***	***Dados***
0x010f	Fabricante da câmera	ascii string	Identificação do fabricante
0x0110	Modelo	ascii string	Descrição do modelo do equipamento
0x0132	Data/Hora Modificação	ascii string	Data e hora de última modificação. O formato utilizado é "YYYY:MM:DD HH:MM:SS".
0x9003	Data Hora Original	ascii string	Data e hora que a imagem foi capturada.
0x9209	Flash	unsigned short	'1' significa que o fash disparou e '0' que o mesmo não foi utilizado.

Tabela 01: Identificadores de algumas informações disponíveis no cabeçalho EXIF

A visualização destes identificadores no arquivo depende do alinhamento de bytes em uso. A maior parte das câmeras usa alinhamento Intel no interior do cabeçalho EXIF, fato que faz com que os identificadores apareçam invertidos no arquivo. O alinhamento utilizado é informado logo após a string "EXIF" no cabeçalho do arquivo: caracteres "II" significam alinhamento Intel e "MM" alinhamento Motorola (Figura 03).

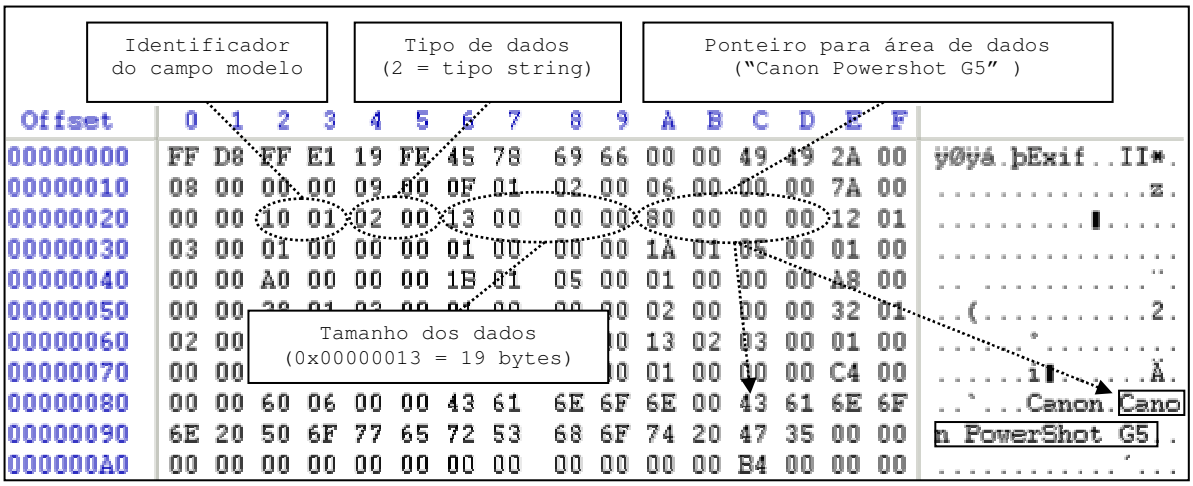


Figura 05: Inspeção do campo registro de modelo da máquina fotográfica utilizada

4. SISTEMAS DE ARQUIVOS

Para que se compreenda a extensão das atividades desenvolvidas pelos peritos durante os exames, é necessário traçar algumas considerações a respeito da organização de arquivos em computadores.

Os arquivos armazenados num disco rígido necessitam estar organizados de forma estruturada. Se assim não estivessem, seria impossível recuperar as informações gravadas. Esta organização é implementada através de uma estrutura denominada Sistema de Arquivos.

Um Sistema de Arquivos é o método e a estrutura de dados que um sistema operacional utiliza para administrar arquivos em um disco ou partição, ou seja, a forma pela qual os arquivos estão organizados em um disco [RIC 1999].

Os sistemas de arquivos encontrados com mais freqüência são os denominados de FAT (e sua variação FAT32) e NTFS, ambos empregados pela família Windows [MIC 03]. Sistemas Linux costumam empregar EXT2, EXT3 e REISERFS.

O que diferencia estes sistemas entre si? Justamente a maneira como as pequenas unidades que compõem o disco rígido, os setores, são inter-relacionados para formar arquivos.

Mas todos têm em comum a existência de duas áreas distintas: uma área de índice ou diretório, onde são registrados os nomes dos arquivos, bem como outras informações tais como data de criação e acesso, usuário que criou o arquivo, atributos de segurança etc; e outra área de dados, onde os arquivos propriamente ditos residem.

O mais importante a ser compreendido é a dinâmica de um sistema de arquivos: quando um arquivo é apagado, o seu conteúdo não é removido; apenas o nome é removido da área de índices. A área que efetivamente armazena o conteúdo do arquivo não é imediatamente sobrescrita ou apagada, nem mesmo em um processo de formatação completa do disco. Durante um certo intervalo de tempo, que pode ser longo, o conteúdo do arquivo pode ser recuperado de forma parcial ou total. A recuperação arquivos apagados é uma riquíssima fonte de informação [FEL 2003].

No caso em questão, o disco rígido analisado apresentava o sistema de arquivos FAT32, onde os dados referentes à posição física dos arquivos, dentre outros, são armazenados em uma área específica do disco, denominada Tabela de Alocação de Arquivos. Quando um arquivo é excluído, os dados referentes à localização do arquivo são apagados da Tabela de Alocação de Arquivos e o espaço antes alocado é marcado como "disponível" [JON 02]. A informação não é destruída, a menos que a região onde está armazenada seja sobrescrita.

Ao gravar novos arquivos no disco rígido, o sistema operacional aproveita qualquer espaço marcado como disponível. Assim, um novo arquivo pode ser gravado tanto sobre um anteriormente apagado quanto em um ponto disponível qualquer da mídia.

Existem ferramentas capazes de recuperar arquivos excluídos que não foram sobrescritos, bem como ferramentas próprias para sobrescrever o espaço ocupado por arquivos que se deseja excluir de forma permanente, destruindo a informação.

5. OS EXAMES EFETUADOS

A metodologia adotada para exames desta natureza pode ser resumida em dois passos principais:

1 - Duplicação do conteúdo dos discos rígidos presentes para preservação do material questionado. Todos os exames são realizados sobre a cópia.

2 - Seleção do material relevante através de análise do conteúdo disponível. Esta análise deve englobar não apenas os arquivos diretamente acessíveis como também os previamente apagados e que ainda se encontram gravados no disco.

Uma das características em casos como este é o elevado número de imagens com conteúdo pornográfico encontrado. Entretanto, durante os exames iniciais, ficou evidente a ausência de imagens desta natureza. Inclusive com a utilização de ferramentas de recuperação de arquivos que trabalham sobre as informações constantes nas cópias da tabela de alocação de arquivos do sistema FAT32, nenhum material relevante foi recuperado.

Constatou-se que o sistema operacional havia sido recentemente instalado, provavelmente na tentativa de ocultar vestígios. A data de criação da pasta que abriga os arquivos do sistema operacional Windows era de apenas uma semana antes da apreensão. Este fato justificou uma atenção mais especial, uma vez que não se tratava de um equipamento novo.

O próximo passo foi efetuar uma busca completa no disco, mas agora utilizando ferramentas de recuperação de conteúdo baseadas em assinaturas de arquivos. Este processo envolve ignorar a área de diretórios e efetuar uma leitura seqüencial de todos setores do disco em busca de seqüências binárias que representem um arquivo digital de formato conhecido. Como visto anteriormente, os arquivos JPG iniciam com a seqüência "0xFFD8" e terminam com "0xFFD9".

Um processo deste tipo normalmente produz uma grande quantidade de arquivos, classificados de acordo com seu tipo, ou seja, formato de reconhecimento. No caso específico, foram recuperadas muitas imagens, sendo um grande percentual destas de cunho pornográfico.

Muitos dos arquivos encontrados apresentavam o formato característico de câmeras digitais (JPG/EXIF). Este também foi um ponto extremamente relevante para as análises, pois normalmente as imagens simplesmente coletadas na Internet não estão neste formato estendido, mas sim no formato JPG comum, apresentando um taxa de compressão mais elevada para reduzir o tamanho do arquivo e facilitar sua divulgação através da rede.

A inspeção das informações armazenadas nestes arquivos de fotografias encontrados possibilitou a identificação de uma máquina digital de modelo específico. Diversas das imagens encontradas aparentavam ser caseiras e retratavam cenas pornográficas envolvendo o suspeito e crianças/adolescentes distintas.

Com base nas informações disponibilizadas no interior dos arquivos partiu-se então para o agrupamento das imagens que compartilhavam características da máquina fotográfica geradora. Ao final deste processo foi possível separar as imagens recuperadas em dois grandes grupos:

- Imagens coletadas muito provavelmente através da Internet e que não apresentavam características de semelhança entre si.

- Fotografias geradas por um modelo específico de máquina digital que apresentavam cenas explícitas de exploração sexual infantil envolvendo o próprio acusado e apresentando semelhanças marcantes de repetição de ambientes e de objetos que na verdade retratavam a residência do envolvido.

O resultado final da análise destacou a existência de mais de 1500 fotografias pornográficas geradas pelo mesmo tipo de máquina, quase todas no mesmo ambiente e com o acusado retratado em boa parte delas.

6. CONCLUSÕES

O exame de equipamentos em informática obriga os analisadores, na maioria das vezes, a lidar com um volume muito grande de informações. A quantidade de arquivos normalmente encontrada durante a análise de um microcomputador atual é extremamente elevada, podendo atingir facilmente o número de 100.000 arquivos.

Um ambiente como este torna proibitiva uma análise visual ou manual de conteúdo sob pena de impor o prazo de vários meses para conclusão de cada exame efetivado. Por outro lado, uma análise superficial pode não produzir resultados satisfatórios, desviando a análise técnica de sua função principal.

No caso específico tratado neste artigo, o conhecimento técnico a respeito do armazenamento de imagens geradas por máquinas fotográficas digitais garantiu o sucesso do trabalho de análise por diversas razões, entre as quais:

- possibilidade de recuperar imagens que não mais estavam registradas no sistema de arquivos;
- descoberta do material realmente relevante, restringindo o ambiente de análise e facilitando a interpretação posterior dos resultados obtidos na perícia;
- separação entre o material produzido pelo suspeito e aquele coletado da Internet;
- identificação do instrumento utilizado para geração das imagens;
- possibilidade de identificar diversos casos de abuso sexual, uma vez que foram encontradas fotografias de inúmeras vítimas e de diversas datas.
- possibilidade de identificação dos locais dos crimes

Em especial na área de exames de informática, o conhecimento específico, técnico e objetivo deve ser sempre buscado pois através dele pode se viabilizar um exame, encontrar informações relevantes não disponíveis naturalmente e contribuir de forma decisiva para o sucesso geral de uma investigação.

7. BIBLIOGRAFIA

[CHA 04] Myths & Facts About JPEG. Chastain, Sue. 2004. Referência: http://graphicssoft.about.com/library/weekly/aa0104jpegmyths.htm

[CPM 04] Comissão Parlamentar Mista de Inquérito – "Exploração Sexual". 2004. Referência: http://www2.senado.gov.br/sf/atividade/Comissoes/consComCPI.asp?com=934

[JPG 04] The Official JPEG Home Page. 2004. Referência http://www.jpeg.org.

[FEL 03] "Email and Other Eletronic Data: Treasure Troves of Evidence". Feldman, Joan E.. 2003. Referência: http://www.forensics.com/pdf/Email.pdf

[MIC 03] Microsoft Corporation. Visão Geral dos Sistemas de Arquivos FAT, HPFS e NTFS. 2003. Referência http://support.microsoft.com/default.aspx?scid=kb;EN-US;100108

[JEI 02] JEITA – Japan Electronics and Information Technology Industries Association. Exchangeable image file format for digital still cameras: Exif Version 2.2. April. CP-3451. 2002.

[JON 02] Jonathan Fox 2000-2002. FAT System Guide. 2002. Referência: http://home.freeuk.net/foxy2k/disk/disk1.htm

[RIC 99] "O que é um sistema de arquivos?", Ricardo Soares Guimarães. 1999. Referência: http://www.li.facens.br/gas/node43.html

LISTA DE AUTORES