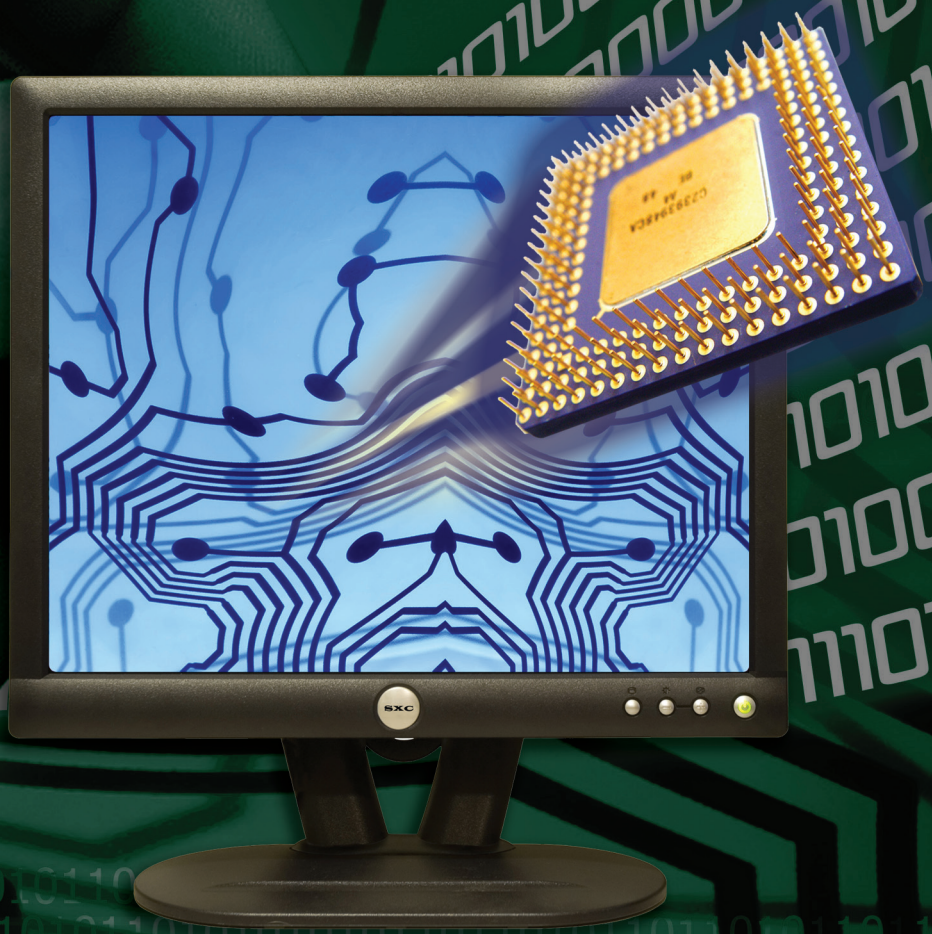
PROCEEDINGS OF

THE INTERNATIONAL CONFERENCE OF FORENSIC COMPUTER SCIENCE

ICoFCS 2006

WWW.ICOFCS.ORG



Number 1, Volume 1, 2006

ISSN 1980-1114

Departamento de Polícia Federal
Diretoria Técnico-Científica
Instituto Nacional de Criminalística

Presidente da República
Luiz Inácio Lula da Silva

Ministro da Justiça
Márcio Thomaz Bastos

Diretor-Geral
Paulo Fernando da Costa Lacerda

Diretor Técnico-Científico
Geraldo Bertolo

Diretora do Instituto Nacional de Criminalística
Zaíra Hellowell

Serviço de Perícias em Informática
Paulo Quintiliano da Silva

Procedings of the First International Conference on Forensic Computer Science Investigation (ICoFCS'2006) / Departamento de Polícia Federal (ed.) -
Brasília, Brazil, 2006, 124 pp. - ISSN 1980-1114

ISSN 1980-1114

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
Zaíra Hellowell
Diretora do Instituo Nacional de Criminalística

Comitê Organizador

Paulo Quintiliano da Silva
Chefe do Serviço de Perícias em Informática

Marcelo Caldeira Ruback
Perito Criminal Federal

Norma Rodrigues Gomes
Perito Criminal Federal

Helvio Pereira Peixoto
Perito Criminal Federal

Antônio Carlos Mesquita
Presidente da APCF

Comitê Revisor

Galileu Batista
João Paulo Botelho
Thiago Cavalcanti
Sérgio Fava
Ricardo Galvão
Norma Gomes
Luis Gustavo Kratz
Luciano Kuppens
Vinicius Lima
José Linhares Silva
Frederico Mesquita
Helvio Peixoto
Paulo Quintiliano da Silva
Cris Rocha
Marcelo Ruback
Marcelo Silva
Murilo Tito
Bruno Werneck

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) 3346-9481

TEMAS DA CONFERÊNCIA

Tema I Crimes no espaço cibernético

01 Exploração sexual de crianças pela Internet
02 Fraudes contra entidades financeiras
03 Terrorismo cibernético
04 Divulgação de informações criminosas por meio da Internet.
05 Outros crimes praticados no espaço cibernético

Tema II Direito Eletrônico

06 Legislação brasileira de crimes cibernéticos
07 Legislação internacional e comparada de crimes cibernéticos

Tema III Cooperação policial internacional

08 Atuação das redes de cooperação policial internacional
09 Alternativas para a melhoria da cooperação policial internacional

Tema IV Robot Networks (Botnets)

10 Prevenção e detecção de botnets
11 Monitoramento de botnets

Tema V Tecnologias correlatas aplicadas

12 Criptologia
13 Biometria
14 Segurança de Rede
15 Redes Neurais Artificiais
16 Reconhecimento de Padrões
17 Processamento de Sinais
18 Prevenção e Detecção de Intrusão
19 Processamento de Imagens
20 Análise de Imagens
21 Visão Computacional
22 Machine Learning

SESSÕES TÉCNICAS - ARTIGOS

A Perícia de Informática na Polícia Federal

Paulo Quintiliano da Silva

Abstract — **Este artigo relata a evolução da perícia de informática na Polícia Federal brasileira, incluindo um histórico da evolução do quadro de peritos de informática e da criação da unidade forense de crimes cibernéticos. Descreve a trajetória internacional da unidade e a legislação interna que a regulamenta. Relata a história das conferências, das publicações científicas e treinamentos, bem como o desenvolvimento de ferramentas forenses pelos peritos criminais federais de informática da Polícia Federal.**

Index Terms — **Polícia Federal, legislação, perícia.**

I. Introdução

A perícia de Informática, no âmbito da Polícia Federal, teve início em 01/11/1995, com a nomeação dos 3 primeiros peritos criminais federais de Informática, após sua aprovação em todas as fases do concurso público. No ano seguinte, outros peritos foram nomeados e também contribuíram muito para a criação da perícia de Informática no âmbito da Polícia Federal. A partir daí, foram elaborados os primeiros laudos de Informática pelos peritos da área. Inicialmente não havia uma unidade específica e nem uma doutrina ou procedimentos especializados.

Em 1996 e 1997, a perícia de Informática, por meio dos peritos Quintiliano, Marcelo Gomes e Walber, realizou um trabalho de grande importância, até hoje considerado um dos maiores feitos da perícia de Informática, levando todos os três a receberem elogios da Direção-Geral pelo trabalho. Trata-se do "Caso Banco Nacional", em que os peritos trabalharam muitos meses nos exames periciais. Os equipamentos questionados eram *mainframes* IBM. Foram examinados milhares de programas nas linguagens *Cobol* e *Easytrieve*, dezenas de aplicativos da instituição, milhões de registros armazenados nesses sistemas e cerca de um bilhão de registros contábeis dos aplicativos da contabilidade do banco. O material estava armazenado em cerca de cinqüenta mil cartuchos magnéticos de ambiente *mainframe*. Ao final, os peritos de informática conseguiram comprovar a ocorrência das fraudes, por meio da análise dos vestígios encontrados nos programas e nos dados. Os peritos de Informática também apoiaram os peritos contadores Bertolo e Cupertino, na conversão dos dados dos cartuchos magnéticos para ambiente *MS-Windows* e na filtragem e disponibilização desses dados em aplicativos específicos desenvolvidos pelos peritos de informática, com facilidades de consultas e emissão de relatórios, que serviram de anexos aos laudos contábeis.

Nos anos seguintes, centenas de outros casos foram trabalhados pelos peritos, alguns também de grande relevância e repercussão nacional. Foram feitos exames periciais para apuração de praticamente todos os crimes da competência federal. Em decorrência dessa atuação forte e também da grande demanda por exames periciais, a perícia de informática, embora seja ainda relativamente nova, hoje certamente já é considerada uma das áreas mais importantes da criminalística da Polícia Federal. Essa conquista também decorre do apoio recebido da direção, do aumento do número de peritos de informática, bem como do altíssimo nível técnico dos profissionais que estão sendo nomeados e da atuação dos peritos mais antigos.

Paulo Quintiliano, Chefe do Setor de Perícias de Informática do Departamento de Polícia Federal, Edifício INC, SAIS Quadra 07 Lote 23 Brasília – DF, CEP: 70610-200, Brasil (e-mail: quintiliano.pqs@dpf.gov.br).

II. Evolução quantitativa da perícia de Informática

No final de 1996, a Polícia Federal já contava com 11 peritos de informática. Em 1999, 6 novos peritos foram nomeados. Nessa época a perícia de informática já possuía uma doutrina e procedimentos bem consolidados. No ano de 2002, o quadro aumentou ainda mais. No final de 2003, a perícia de Informática da Polícia Federal já contava com 40 profissionais.

No ano de 2005, foi realizado concurso público para a admissão de 105 novos peritos criminais federais de informática. Nesse mesmo ano, foram nomeados os primeiros profissionais da área aprovados no concurso. Em 2006, novos peritos de informática foram nomeados. Até o final deste ano, o total de peritos, com atuação na área, será cerca de 140, lotados em Brasília e nas outras capitais, para o atendimento das necessidades de todo o país.

III. Unidade de crimes cibernéticos

Em 1996, foi criada a Unidade de Perícia de Informática da Polícia Federal. Inicialmente ela funcionou de maneira informal, para depois ser instituída formalmente no organograma da Polícia Federal.

A Unidade já teve outros nomes, o primeiro foi SACC (Serviço de Apuração de Crimes por Computador). A segunda sigla utilizada foi SECC e, depois, SINF. Em 2003, recebeu a denominação atual: SEPINF (Serviço de Perícias de Informática).

No ano de 2006, por meio de Instrução Normativa, foi criado o GEBAC (Grupo Especial de Busca e Apreensão de Computadores), ligado aos peritos de informática. O objetivo

do grupo é apoiar a busca e apreensão de equipamentos e de outros recursos de informática em locais de crime.

IV. Contatos Internacionais

A partir de 1996, os peritos de Informática começaram a estabelecer contatos com vários outros países, participando de conferências e de treinamentos específicos, tendo como um dos principais objetivos o estabelecimento e a consolidação de sua doutrina de elaboração de exames periciais. O primeiro contato internacional da perícia de informática ocorreu em fevereiro de 1996, quando o perito Quintiliano participou da conferência "The International Organization on Computer Evidence (IOCE)", em Melbourne, Austrália. A partir de então, muitos peritos de Informática têm participado de eventos e cursos internacionais, inclusive como instrutores e palestrantes.

A perícia de informática logo percebeu a grande importância de sua conexão com a comunidade internacional voltada para o combate aos crimes cibernéticos. Esses crimes, como se sabe, não têm fronteiras. Dessa forma, a melhor forma de combatê-los, principalmente quando possuem efeitos internacionais, é a cooperação direta entre as forças policiais dos países envolvidos na situação [3, 4, 5, 6]. Nesse sentido, a perícia de Informática está conectada às principais comunidades internacionais de policiais, voltadas para o combate aos crimes cibernéticos.

V. Legislação interna

Em 2004, a perícia de Informática concebeu e elaborou uma minuta de Instrução Normativa (IN), com o objetivo de regulamentar as atividades da perícia de Informática no âmbito da Polícia Federal. A partir dessa iniciativa, foi publicada a IN 007/2005-DG/DPF. Essa instrução estabelece a obrigatoriedade da presença dos peritos criminais federais de informática no planejamento das operações envolvendo crimes dessa natureza, de modo a permitir que os objetivos sejam atingidos com maior eficiência e eficácia [2].

A perícia de Informática concebeu e elaborou, em 2005, uma minuta de Instrução Técnica (IT), com o objetivo de estabelecer os critérios dos exames da perícia de informática, bem como formalizar a doutrina da perícia de informática da Polícia Federal. A partir desse trabalho, foi publicada a IT 001/2005/GAB/DITEC [1].

Em decorrência dessa legislação interna ser muito recente, os órgãos da Polícia Federal ainda estão em fase de adaptação para que possam observá-la plenamente.

VI. Conferências e publicações científicas

Em setembro de 2004, a perícia de Informática da Polícia Federal realizou a I Conferência Internacional de Perícias em Crimes Cibernéticos (ICCyber 2004), em Brasília. A conferência contou com a presença de mais de 600 participantes de 21 países e teve grande repercussão nacional e internacional. Na mesma semana da ICCyber 2004, foi realizado o I Encontro Nacional dos Peritos Criminais Federais Federais de Informática (I ENPCFI). Nesse encontro foram discutidos vários assuntos afetos à perícia de informática, bem como foram deliberadas importantes decisões com o objetivo de nortear as ações a serem adotadas no âmbito da perícia de informática.

A perícia de informática da Polícia Federal realizou, Em dezembro de 2005, a II Conferência Internacional de Perícias em Crimes Cibernéticos (ICCyber 2005), também em Brasília. Nesse ano, sem desprestigiar os outros temas, a conferência teve o foco principal voltado para os ataques de *botnet*, uma das maiores ameaças do espaço cibernético na atualidade. Houve palestras e treinamentos específicos sobre o assunto. A conferência contou com a participação de palestrantes e conferencistas de vários países.

Atualmente, em 2006, a perícia de informática da Polícia Federal do Brasil, com o objetivo de consolidar a posição como referência mundial em sua área de atuação, estabelece algumas ações de grande importância: a criação da revista científica IJoFCS; a realização da conferência científica internacional ICoFCS; e a fundação da editora Forensic Press.

A revista científica internacional "The International Journal of Forensic Computer Science (IJoFCS)" tem como principal objetivo atrair e motivar a comunidade científica atuante na área da Ciência da Computação para um direcionamento de suas pesquisas à Ciência da Computação Forense, de modo a acelerar o seu desenvolvimento e permitir que as polícias tenham novas ferramentas para o combate aos crimes cibernéticos, possibilitando à sociedade maior segurança nessa área.

"The International Conference on Forensic Computer Science (ICoFCS)" é uma conferência internacional de Ciência da Computação Forense que terá sua primeira edição realizada juntamente com a ICCyber, no mesmo local e período. A ICoFCS absorve a vertente mais científica da ICCyber, somente serão publicados em seus anais os artigos submetidos e aceitos pela Banca Examinadora, composta por peritos de informática e por outros cientistas da computação ligados às universidades e aos centros de pesquisas.

Em 2006, com a finalidade de produzir e de divulgar os conhecimentos gerados pelos peritos de Informática e por outros cientistas da computação, a perícia criminal federal de informática fundou a editora "Forensic Press", que será responsável pela publicação do IJoFCS; dos anais da ICCyber e da ICoFCS; e de outros conhecimentos científicos produzidos pelos peritos de informática e por outros cientistas da área da Ciência da Computação Forense.

Nos próximos anos, pretende-se fortalecer e consolidar as ações da perícia criminal federal de informática, relativas às conferências, à revista científica, ao curso internacional de computação forense e à editora, pois são veículos importantes para a produção e a divulgação do conhecimento científico na área da Ciência da Computação Forense. A partir desse conhecimento produzido, pretende-se desenvolver e aperfeiçoar ferramentas úteis para apoiar os exames periciais de informática e o combate aos crimes cibernéticos de uma

forma geral.

VII. Curso Internacional de Computação Forense

O treinamento internacional em Ciência da Computação Forense, "The International Training of Forensic Computer Science (IToFCS)", foi idealizado pela Perícia Criminal Federal de Informática, com apoio da JICA/Japão, para que sejam ministrados cursos para peritos e investigadores brasileiros e de outros países, de modo a disseminar a doutrina e os conhecimentos acumulados em mais de dez anos de trabalho.

VIII. Ferramentas forenses desenvolvidas pelos peritos

O "Assistente de Análises Periciais (AsAP)" foi concebido e desenvolvido pelos peritos criminais federais de informática, com o objetivo de dar maior celeridade aos exames periciais em mídias de armazenamento computacional. Praticamente em todas as operações da Polícia Federal são apreendidas dezenas ou centenas de discos rígidos (HD) e de outras mídias, visto que os criminosos estão, cada vez mais, fazendo uso de computadores e de outros recursos de informática em suas atividades criminosas [3, 4, 5, 6]. A perícia de informática poderia se tornar um entrave nas investigações, visto que não poderia conseguir atender às demandas atuando da forma tradicional, com o uso de softwares forenses convencionais. Assim, para dar celeridade a esses importantes exames periciais, a perícia de informática da Polícia Federal concebeu e desenvolveu o AsAP, que possibilita diminuir em até 80% o tempo de elaboração dos exames periciais em mídias de armazenamento computacional.

Serão direcionados muitos esforços no aperfeiçoamento do AsAP, outras versões com novas e importantes funcionalidades serão geradas, de forma a facilitar e a otimizar os exames perícias em mídias de armazenamento computacional.

IX. Conclusão

A Perícia Criminal Federal de Informática tem uma história de 11 anos na Polícia Federal. Em 1995, somente existiam 3 peritos, mas, ao final deste ano, cerca de 140 peritos de informática estarão atuando diretamente nos exames periciais da área. A perícia de informática evoluiu muito, hoje já conta uma doutrina consolidada, procedimentos e padrões estabelecidos. Possui veículos de produção e de divulgação do conhecimento científico gerado pelos peritos e por outros cientistas da computação, representados pelas conferências, pela revista científica, pelo curso internacional e pela editora.

Nesse cenário, certamente a Perícia Criminal Federal de Informática vem procurando atingir um de seus maiores objetivos, consolidar-se como referência mundial em sua área de atuação.

References

[1] Polícia Federal, Instrução Técnica Nº 001/2005/GAB/DITEC, de 10 de outubro de 2005. Dispõe sobre a padronização de procedimentos e exames no âmbito da perícia de informática, 29 pp, 2005.

[2] Polícia Federal, Instrução Normativa Nº 007/2004-DG/DPF Brasília/DF, 15 de outubro de 2004. Estabelece as diretrizes de atuação e os procedimentos no âmbito das perícias em crimes por computador, 3 pp, 2004.

[3] Silva, Paulo Quintiliano da, "Crimes Cibernéticos no Contexto Internacional", In: Anais do XIII Congresso Mundial de Criminologia, Rio de Janeiro-RJ, Brasil, 2003, 8pp.

[4] Silva, Paulo Quintiliano da. "Perícias em Crimes Cibernéticos", In: Anais do XVII Congresso Nacional de Criminalística, Londrina-PR, Brasil, 2003, 8pp.

[5] Silva, Paulo Quintiliano da. "Crimes Cibernéticos e seus Efeitos Multinacionais", In: Revista Perícia Federal, Brasil, 2004, 6pp.

[6] Silva, Paulo Quintiliano da. "Cooperação Policial Internacional no Combate aos Crimes Cibernéticos", In: Proceedings of ICCyber'2004 – First International Conference on Cyber Crime Investigation, 7pp, 2004.

Crimes cibernéticos e seus efeitos internacionais

Paulo Quintiliano da Silva
Serviço de Perícia de Informática da Polícia Federal
Email: quintiliano.pqs@dpf.gov.br

***Abstract* — Neste artigo, os crimes cibernéticos são contextualizados no cenário internacional, apresentando as principais características desses crimes e as dificuldades encontradas em sua investigação. São abordadas as iniciativas dos principais organismos internacionais referentes ao enfrentamento desses crimes. As alternativas de combate a esses crimes, a reestruturação das agências policiais e a cooperação policial internacional direta entre essas agências são apresentadas.**

***Index Terms* — Crimes cibernéticos, organismos internacionais, perícia, agências policiais.**

I. Introdução

UMA das características dos crimes cibernéticos que mais dificulta as investigações é o fato de não existirem fronteiras no espaço cibernético. 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. Além disso, os vestígios que poderiam permitir a identificação e a localização dos autores desses crimes podem se perder definitivamente em pouco tempo. O criminoso pode estar em qualquer parte do planeta e, mesmo assim, pode conseguir atingir alvos em quaisquer localidades, por mais longínquas que estejam. Na verdade, o espaço cibernético conseguiu juntar virtualmente todo o planeta, transformando-o numa teia acessível por todos, de qualquer parte. Aproveitando-se desse fato, muitas quadrilhas que atuavam da forma tradicional estão migrando suas atividades criminosas para o espaço cibernético, por julgarem correr menos riscos e por obterem maiores ganhos financeiros em menor espaço de tempo. Esses criminosos estão cooptando jovens com conhecimentos de informática para fazerem parte de suas quadrilhas, com atuação na parte mais técnica, que exige maior experiência no assunto [1, 2, 3, 4, 5, 6, 7, 8].

Muitas dessas quadrilhas têm atuação internacional, são compostas por membros residentes em vários países. Usam as técnicas mais modernas e eficazes na consecução de suas atividades criminosas. Eles compartilham informações sem qualquer burocracia, disseminam conhecimentos, descobertas, dados e programas obtidos.

Vários organismos internacionais tomaram, ou estão tomando, medidas sérias para o combate a esses crimes. O G8, grupo dos oito países mais industrializados, criou e mantém a Rede 24x7. O Conselho da Europa criou a Convenção dos Crimes Cibernéticos. A Organização dos Estados Americanos (OEA), a Organização das Nações Unidas (ONU), o Banco Mundial e outros organismos internacionais vêm discutindo o assunto de forma recorrente, gerando grande quantidade de documentos. As agências policiais de todo o mundo estão preocupadas com o assunto e estão tomando as medidas que julgam corretas e pertinentes.

A Rede 24x7 do G8 é bastante ágil, contudo suas ações e abrangência são muito limitadas. Essa rede funciona bem para a solicitação da preservação das informações que poderão ser usadas para a comprovação da materialidade e autoria dos crimes, até que se consigam as necessárias cartas do MLAT (*Mutual Legal Assistance Treaty*) ou Cartas Rogatórias. Contudo, essas cartas demoram muito e por isso não se prestam para serem utilizadas em casos de crimes cibernéticos, pois os vestígios são muito voláteis e podem se perder em pouco tempo. Além disso, em se tratando de crimes cibernéticos, os incidentes acontecem muito rapidamente, necessitando de ações imediatas.

A Convenção dos Crimes Cibernéticos do Conselho da Europa deve dar bons resultados a médio prazo, quando um grande número de nações a tiver ratificado e ela já estiver operando em muitos países. Por enquanto, os resultados práticos dessa convenção ainda são isolados e de pouco expressividade, até mesmo porque sua operação iniciou há muito pouco tempo, com um número reduzido de países, e movimentação no espaço cibernético não muito significativa.

As discussões e os documentos da OEA, da ONU, do Banco Mundial e de outros organismos internacionais ainda não geraram resultados práticos que pudessem contribuir de forma efetiva para o combate aos crimes cibernéticos. Com certeza, as iniciativas desses organismos internacionais são de grande relevância, a expectativa é surjam bons resultados a partir dessas ações.

II. Situação atual

Considerando os procedimentos rotineiros utilizados de forma geral, normalmente são necessárias Cartas Rogatórias para 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

são concluídos, os provedores de serviços de Internet responsáveis pela guarda dos dados já liberaram as mídias magnéticas que continham os dados de interesse, tornando os vestígios perdidos.

Sabe-se que grande parte dos provedores de serviços de Internet mantém as suas cópias com os *logs* dos acessos e demais vestígios por, no máximo, noventa dias e, às vezes, por período ainda menor, visto que ainda não existem leis que regulamentam suas atividades, obrigando-os a preservarem os dados por mais tempo. Considerando 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 em que criminosos brasileiros, fazendo uso do espaço cibernético, atacaram sítios de entidades governamentais estrangeiras, causando danos sérios. Quando o processo chega no momento de serem realizadas as investigações e as perícias, já se passaram seis meses, um ano ou até mais, não havendo como descobrir a autoria do crime, pois os dados já se perderam.

De forma semelhante, quando são solicitados dados que estão armazenados em provedores de serviços de Internet no exterior, para efeito de identificação e de localização de suspeitos, a solicitação muitas vezes sequer chega a ser feita, em decorrência da grande morosidade dos procedimentos. Isso acontece porque, quando se trata de crimes cibernéticos, não é possível esperar os prazos exigidos pelos procedimentos feitos por meio das Cartas Rogatórias.

Houve casos em que foram feitas tentativas junto aos provedores estrangeiros de serviços de Internet com representação no Brasil, no sentido de buscar informações de criminosos brasileiros, com base em ordens judiciais. A informação recebida foi de que os dados estavam 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.

III. Cenário dos crimes cibernéticos nos próximos anos

O espaço cibernético está sendo utilizado cada vez mais para a prática de crimes. A tendência assinalada é de crescimento das atividades criminosas por meio do espaço cibernético. Dessa forma, questiona-se como seria o cenário mundial no ano de 2020, a respeito desse tipo de atividade criminosa. Para tentar responder a essa questão, é importante lembrar que há 15 anos esse tipo de crime era muito incipiente ou quase inexistente, e que nesse espaço de tempo ele experimentou um vertiginoso crescimento e um aperfeiçoamento incomparáveis.

Pode-se inferir que ocorrerá daqui a 15 anos um cenário em que os criminosos terão muito mais conhecimentos e habilidades no uso da informática e na prática dessa modalidade de crime, visto que esses infratores nasceram ou terão nascido na era da cibernética e da inclusão digital. Além disso, os pacotes de softwares utilizados para a prática dos crimes estão sendo comercializados pela Internet a custos acessíveis, ou que até podem ser obtidos gratuitamente. Assim, é possível prever que nesse cenário esses criminosos deverão fazer uso da Internet, de computadores e de outros recursos da Informática como ferramentas para a prática de suas atividades criminosas.

Diante do quadro assinalado, de um lado as autoridades governamentais, responsáveis pela persecução penal dessas atividades criminosas e sensíveis aos problemas cibernéticos, devem adotar, desde já, medidas eficazes para o combate dessas condutas, pois o espaço cibernético poderá se tornar muito inseguro, vulnerável e de baixa confiabilidade, comprometendo o avanço das atividades responsáveis que vêm sendo conduzidas por meio da Internet, tanto nos campos científico e comercial, como na área de governo.

De outro lado, as polícias têm que se preparar adequadamente, por meio do treinamento de seus policiais, da aquisição de ferramentas, da formação de doutrinas, da cooperação policial internacional e da adequação e modernização de sua estrutura de combate aos crimes cibernéticos, de forma a se tornar uma única grande unidade especializada em investigação de crimes cibernéticos, pois praticamente todos os crimes estarão fazendo uso do espaço cibernético, de computadores e de outros recursos da informática para a prática de suas condutas criminosas [4, 5, 6, 7, 8].

Nesse sentido, urge que os policiais, no mais curto prazo possível, sejam habilitados, por meio de treinamentos específicos, a investigar os crimes de suas respectivas áreas de competência também quando praticados dentro do espaço cibernético. As agências policiais, da mesma forma, devem buscar procedimentos céleres de cooperação policial internacional, com a utilização de redes conectando o maior número possível de países, que possibilitem o estabelecimento de intercâmbio de informações de investigação, em consonância com a velocidade que experimentam os crimes cibernéticos.

Dessa forma, poder-se-á garantir uma atuação policial efetiva no combate aos crimes cibernéticos, mesmo nos casos em que os efeitos dos crimes são espalhados em vários países, estando os criminosos muitas vezes localizados em países distintos e distantes entre si, de forma organizada em quadrilhas internacionais.

IV. Estrutura das agências policiais

Os chamados “crimes cibernéticos” normalmente podem ser enquadrados em crimes já tipificados na legislação penal brasileira, pois estão sendo cometidos os crimes já existentes, apenas utilizando a informática e o espaço cibernético como

uma ferramenta adicional às atividades criminosas. Um exemplo típico dessa assertiva é a ação do estelionatário, que é muito criativo e sempre encontra no espaço cibernético uma fonte inesgotável de possíveis vítimas.

Observa-se que os crimes cibernéticos estão ocorrendo dentro de várias áreas de atuação da polícia. Por meio do espaço cibernético, são cometidos crimes de tráfico de drogas, de exploração sexual de crianças, de lavagem de dinheiro, de colarinho branco, de dano, de falsificação de documentos públicos, de estelionato, de apologia de crime ou fato criminoso, crimes fazendários, e muitos outros [8].

Vale ressaltar que as atividades criminosas estão fazendo e continuarão a fazer cada vez mais uso da informática e do espaço cibernético na consecução dos objetivos criminosos. Nesse contexto, é possível que em breve chegue o momento em que todas as áreas operacionais das polícias terão que estar aptas a também fazerem as suas investigações no espaço cibernético.

Dessa forma, as várias áreas de atuação das polícias terão que se estruturar para atuarem e investigarem os crimes de suas respectivas competências também quando praticados no espaço cibernético. Isso pode ser feito por meio da criação de setores específicos de repressão aos crimes cibernéticos dentro de cada uma dessas áreas, para que atuem no combate aos crimes de suas competências respectivas, praticados dentro e fora do espaço cibernético.

É importante que todas as áreas de atuação das polícias tenham seus próprios setores de repressão aos crimes cibernéticos, visto que dessa forma certamente serão evitadas possíveis sobreposições de atribuições, pois tais unidades especializadas somente atuariam na repressão dos crimes de suas respectivas competências. Assim, possibilitar-se-ia a especialização dos policiais nos crimes de suas áreas de atuação, bem como seria evitada a duplicidade de esforços e as possíveis invasões de atribuição entre as várias áreas das agências policiais.

Se fosse criado apenas um setor ou uma diretoria de crimes cibernéticos dentro da polícia, esse fato poderia gerar, além da sobreposição de atribuições com relação aos órgãos operacionais das polícias, uma grande concentração de atividades nesses novos órgãos especializados em crimes cibernéticos, podendo até inviabilizar suas atividades, pois é grande o crescimento da incidência de crimes praticados no espaço cibernético ou com a utilização de computadores e outros recursos de informática.

Entende-se que as principais unidades operacionais e centrais das agências policiais devem ser contempladas com treinamentos e ferramentas específicos, preferencialmente à criação de setores formais especializados na repressão aos crimes cibernéticos. Assim, os policiais devem ser habilitados a investigarem os crimes de suas respectivas áreas de atuação também quando praticados com a utilização da informática e do espaço cibernético. Dessa maneira, todas as unidades da polícia poderiam continuar trabalhando em suas áreas de atuação, sem haver sobreposição de atribuições nas investigações e o grupo de policiais especializados em crimes cibernéticos poderia estar inserido numa estrutura formal para a atuação nas investigações dos crimes de suas respectivas competências, quando praticados no espaço cibernético.

Dessa forma, as agências policiais, com o objetivo de enfrentar o cenário previsto neste trabalho, tornar-se-iam uma grande e moderna unidade policial de crimes cibernéticos, preparada para investigar todos os crimes de sua competência, praticados dentro ou fora do espaço cibernético, com ou sem a utilização de computadores e de outros recursos da informática. Estariam preparadas para enfrentar talvez um dos maiores desafios e uma das maiores ameaças da criminalidade neste século XXI. Esses desafios e ameaças estão vindo e continuarão a vir pelo espaço cibernético, estão atingindo e continuarão a atingir alvos de toda a sociedade moderna.

V. Cooperação Policial Internacional Direta

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. As ações de combate aos crimes cibernéticos, principalmente quando dois ou mais países estão envolvidos, não podem esperar os prazos dilatados dos mecanismos convencionais de cooperação internacional. Os mecanismos mais comuns para a busca e a validação de vestígios provenientes do exterior são a tradicional Carta Rogatória, as cartas do *Mutual Legal Assistance Tready* (MLAT) e as solicitações da Rede 24x7 do G8.

A Carta Rogatória precisa passar pelas supremas cortes dos países envolvidos, após a adoção de vários procedimentos morosos, como a tradução juramentada e o encaminhamento de um país para outro, normalmente necessitando de prazos superiores a dois ou três anos para a sua conclusão. Certamente essa medida não se presta para a utilização em casos de crimes cibernéticos, que exigem atuação imediata dos órgãos governamentais [8].

O MLAT, embora possa ser mais célere do que outros mecanismos, também é bastante burocrático e lento. Além disso, o MLAT é um acordo bilateral entre os Estados Unidos e vários outros países. Assim, somente é possível utilizar o MLAT com os Estados Unidos, nos casos em que seja necessária a cooperação com outras nações, esse canal não está disponível.

A Rede 24x7, organizada e mantida pelo *Subgroup on High-Tech Crime* do grupo dos 8 países mais industrializados, identificado como G8, é bastante célere, as comunicações entre os pontos de contatos são feitas por telefone ou por mensagens eletrônicas, garantindo a maior rapidez possível, durante 24 horas por dia e 7 dias por semana. Esse é o espírito da Rede, a partir do qual decorre o seu nome. No entanto, a Rede 24x7 ainda é bastante limitada, tanto em termos de quantidade de países membros (atualmente há pouco mais de 40 países filiados), como de sua reduzida atuação. Hoje, a Rede 24x7 somente se presta para que os países-membro sejam acionados

sejam acionados para solicitarem aos Provedores de Serviços de Internet (PSI) a preservação dos vestígios relativos aos crimes praticados por meio do espaço cibernético, evitando a perda dessas informações. Contudo, para que essas informações realmente sejam obtidas pelo país solicitante, é necessário que o requerimento seja feito por meio de um acordo de cooperação jurídica, como o MLAT, ou por meio de Cartas Rogatórias.

Para tentar minimizar essas adversidades na condução das investigações, propõe-se a adoção da Cooperação Policial Internacional para o Combate aos Crimes Cibernéticos (*International Police Co-operation to Combat the Cyber Crimes – IPCCCC*).

Além do Conselho da Europa, várias outras organizações internacionais, como as Nações Unidas, a Organização dos Estados Americanos (OEA), a União Européia, a *European Police Office* (Europol) e a Interpol, também estão adotando suas medidas visando à cooperação policial internacional para o combate aos crimes cibernéticos.

Dadas as características dessa ação criminosa, em que muitas vezes as suas provas são perdidas em poucos meses ou semanas, para o seu combate efetivo é necessária a cooperação policial 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. 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 todos os vestígios, inviabilizando-se o trabalho da investigação policial.

VI. IPCCCC

O IPCCCC consiste no estabelecimento de cooperação policial internacional, por meio da adoção de mecanismos ágeis no combate aos delitos cibernéticos, especialmente aqueles 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 [8].

No âmbito do IPCCCC, está sendo considerada a necessidade da "nacionalização" das provas produzidas no exterior, por meio dos procedimentos estabelecidos. Essa cooperação policial internacional para o combate aos crimes cibernéticos 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. Para que o IPCCCC funcione em sua totalidade, é necessária a adesão do maior número possível de países, para que essa cooperação se torne universal e possa alcançar todas as localidades conectadas na Internet. As ações e os mecanismos propostos serão adotados principalmente principalmente pelos Grupos Técnicos de cada país, da forma mais ágil possível e com o mínimo de formalidade.

Pode-se considerar a participação da Rede 24x7, organizada e administrada pelo G8, da qual o Brasil é membro. Essa Rede, também conhecida como "G8 24/7 *Computer Crime Network*", já possui pontos de contato, está estruturada em mais de 40 países, e pode ser utilizada na implantação do IPCCCC, com as devidas estruturações e adequações em alguns de seus pontos de contato, quando for o caso. Para tanto, é necessária a existência de policiais especializados em crimes cibernéticos em todos os países participantes, que funcionarão como os pontos de contato da Rede. É importante que os membros desses grupos sejam policiais com formação em Ciência da Computação ou com bastante conhecimento e experiência em 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, de maneira uniforme.

VII. 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 lícitas 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 cooperação policial internacional, por meio dos grupos de cooperação formados pelos órgãos governamentais responsáveis, de modo a ser possível enfrentar com maior probidade essa nova face do crime do século XXI.

Os criminosos estão, dia após dia, migrando suas atividades ilícitas para o espaço cibernético. Observando a tendência evidenciada e discutida neste artigo, em 15 anos, praticamente todos os criminosos estarão fazendo uso do espaço cibernético e/ou de computadores e outros recursos de informática na realização de suas atividades criminosas. Para se conviver nesse ambiente, as polícias têm que se preparar, adaptando-se a essa realidade mutante, para o enfrentamento dessa nova modalidade criminosa.

Neste artigo são propostas duas ações para um combate mais eficiente e eficaz desses crimes: a) modernização das investigações, incluindo o treinamento dos policiais, para que os mesmos possam investigar os crimes de suas respectivas competências dentro do espaço cibernético, bem como a criação de setores especializados na repressão dos crimes cibernéticos dentro da estrutura das várias áreas de atuação das polícias e; b) estabelecimento de cooperação policial internacional, por meio do IPCCCC, especialmente nos casos em que dois ou mais países estejam envolvidos na investigação e/ou na prática dos crimes.

Infere-se que a modernização proposta possibilitará uma ação mais efetiva da polícia, quando serão utilizados policiais

já especializados em suas respectivas áreas de atuação, para que esses próprios especialistas também façam investigações no espaço cibernético. Dessa forma, serão evitadas possíveis duplicações de esforços e invasões de atribuições de uma área em relação às outras.

Quanto à cooperação policial internacional proposta – a IPCCCC –, ela permitirá que as investigações internacionais envolvendo dois ou mais países sejam eficazes e mais agilizadas. Serão evitados procedimentos morosos para a obtenção de vestígios estrangeiros, como as Cartas Rogatórias. O IPCCCC pode possibilitar ações imediatas, em tempos compatíveis com a velocidade que experimentam os crimes cibernéticos, com informalidade e rapidez semelhantes às das ações ilícitas dos criminosos do espaço cibernético.

Dessa forma, as ações propostas neste artigo podem permitir que as agências policiais se antecipem a esse cenário de mudança que as envolve e as limita, possibilitando o enfrentamento dessa modalidade criminosa, no momento adequado.

Referências Bibliográficas

[1] Ashcroft, John, "Electronic Crime Scene Investigarion: A Guide for First Responders", U.S. Department of Justice Office of Justice Programs, 93pp., 2001.

[2] Carrier, Brian, "Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers", In: International Journal of Digital Evidence, Winter 2003, Volume 1, Issue 4, 12pp, 2003.

[3] Cassey, Eoghan, "Error, Uncertainty, and Loss in Digital", In: International Journal of Digital Evidence, Summer 2002, Volume 1, Issue 2, 45pp, 2002.

[4] Silva, Paulo Quintiliano da, "Crimes Cibernéticos no Contexto Internacional", In: Anais do XIII Congresso Mundial de Criminologia, Rio de Janeiro-RJ, Brasil, 8pp., 2003.

[5] Silva, Paulo Quintiliano da. "Perícias em Crimes Cibernéticos", In: Anais do XVII Congresso Nacional de Criminalística, Londrina-PR, Brasil, 8pp., 2003.

[6] Silva, Paulo Quintiliano da. "Crimes Cibernéticos e seus Efeitos Multinacionais", In: Revista Perícia Federal, Brasil, 6pp., 2004.

[7] Silva, Paulo Quintiliano da. "Cooperação Policial Internacional no Combate aos Crimes Cibernéticos", In: Proceedings of ICCyber'2004 – First International Conference on Cyber Crime Investigation, 7pp, 2004.

[8] Silva, Paulo Quintiliano da, "Crimes Cibernéticos sob uma Abordagem Investigativa", Monografia do curso MBA em Gestão de Segurança Pública, FGV, Brasília-DF, Brasil, 60pp, 2005.

Botnets as a Vehicle for Online Crime

Nicholas Ianelli and Aaron Hackworth

Abstract—An analysis of real-word botnets[1] indicates the increasing sophistication of bot[2] malware and its thoughtful engineering as an effective tool for profit-motivated online crime. Our analysis of source code and captured binaries has provided insight about:

- **how botnets are built**
- **what capabilities botnets possess**
- **how botnets are operated**
- **how botnets are maintained and defended**

The purpose of this paper is to increase understanding of the capabilities present in bot malware and the motivations for operating botnets.

I. Motivations for Creating Botnets

Communication, resource sharing, and curiosity have historically been primary motivators for underground research and "hacking." However, as the general public's participation in the internet has expanded, and the percentages of e-commerce and online financial transactions have grown, online attackers have shifted their focus from curiosity to financial gain. To accomplish this goal, they vigorously pursue access to information and capacity.

A. Information gathering

Most computer systems contain valuable information about the users or business activities they support. Even when the existence and value of information is not clear to a system's users, the attackers know exactly where it is located, how to extract it, and how to profit from it.

When systems are compromised by malicious code, whether through remote attack or by tricking the user into installing malware, the attacker gains access to the information and system resources available to the user. In many cases this equates to administrator-level privileges and allows the attacker access to personal or confidential information such as usernames, passwords, email contacts, financial information or trade secrets. Access is not limited to persistent data available on the hard drive or stored in the registry; it can also include transient data, such as screen shots, keystrokes, and network traffic observed on connected networks.

Once the attackers have the information, they turn a profit by using, trading, or selling it. This creates a large problem for individual users and can also have vast negative impact on an organization and possibly the public if valuable intellectual property is stolen, such as customer databases, partner information, or other sensitive data.

When an organization's data has been stolen, it is commonly used to perpetrate future attacks against the organization and its individual members. These attacks include:

- extortion
- social engineering
- reuse of system access credentials
- attempts to gain additional access to other organizational resources

Many organizations are dedicating additional resources towards system security, staffing, technologies and other defensive resources to protect their information and computer systems. Although this may help minimize the risk of successful compromises it does not eliminate it. Determined attackers understand that while there may be significant barriers to entry, the amount and value of information provided through a successful organizational compromise could have a significantly higher return on investment than that of a home user's system. On the other hand, despite the lower per-compromise payoff, some attackers are attracted to the systems of individual internet users because of the ease of compromise and volume of vulnerable systems.

B. Acquiring capacity

Attackers also value computing resources and bandwidth. Mass market end-user systems continue to drop in price and improve in processing speed and storage capacity. This trend, coupled with migration toward high-bandwidth broadband connections [2005 Bandwidth Report], makes low security, large capacity systems readily available and ripe for harvesting.

Collecting and controlling a large group of these systems provides attackers and their collective associates (i.e., crews) enormous power. For instance, they can use this power

Manuscript received October 18, 2006.

Nicholas Ianelli is an Internet Security Analyst for the CERT Coordination Center.

Aaron Hackworth is an Internet Security Analyst for the CERT Coordination Center.

[1] Botnets are collections of computers infected with malicious code that can be controlled remotely through a command and control infrastructure.

[2] A bot is an individual computer infected with malicious code that participates in a botnet and carries out the commands of the botnet controller.

collectively to execute a distributed denial of service (DDoS) attack. By creating large, geographically dispersed botnets, attackers have been able to launch DDoS attacks from valid source addresses, making them increasingly difficult to shutdown or filter. This capability has been used in attempt to extort money from online businesses [2005 Pappalardo and Messmer].

Attackers can also use this capacity to distribute warez,[3] set up phishing sites, launch spam campaigns, etc. Because the capacity belongs to other organizations and users, the attackers' cost and risks for engaging in these activities is minimal.

II. Techniques for Creating Botnets

A. Building from scratch

Building a botnet requires only minimal technical skill. With some exceptions, the attacker community is ready and willing to share their knowledge with almost anyone interested in learning. A wealth of information is available for download explaining how to compromise systems, where to obtain packaged exploits, and simple command-line and GUI-run exploit frameworks. Many internet relay chat (IRC) channels offer training sessions and advice to attackers just starting out. This kind of knowledge sharing helps the underground community thrive.

When creating a botnet, the attacker needs vulnerable systems to exploit. Detailed lists of IP ranges (netblocks) are shared amongst the underground community including:

- netblocks ripe with vulnerable systems
- netblocks that are heavily monitored and should be avoided
- netblocks that are unallocated or un-routable
- netblocks that are allocated to certain types of organizations (for example colleges or government)

Because of the increasing number of network-connected computer systems, attackers can be more selective about the systems they target. For instance, "always-on" broadband connections make a better target because of their bandwidth capacity. Attackers can leverage this capacity to assemble powerful botnets more quickly. Therefore, attackers may target broadband systems because they yield a higher return on investment. A single broadband system could provide the same bandwidth as up to seventy dialup systems.

Educational address space (.edu) is another popular target. Because these systems are often poorly secured, have large storage capacities, and feature fast network connections from large backbone providers, they make an ideal target for warez servers. Military and government systems are also popular targets for various reasons, including capacity, access to information and other resources, and bragging rights among the underground community. While some attackers shy away from .mil and .gov systems, others will pay top dollar for access to these resources.

B. Vulnerability exploitation

One way computers are attacked is through software vulnerabilities. Software vulnerabilities may also be leveraged incrementally to compromise a system. Thus, an attacker may combine several vulnerabilities to gain control of a computer because a single vulnerability in and of itself may not provide the level of access desired.

Some of the more commonly exploited vulnerabilities used to spread bot malware have been documented for quite some time and include:

- VU#568148: Microsoft Windows RPC vulnerable to buffer overflow
- VU#753212: Microsoft LSA Service contains buffer overflow in DsRolepInitializeLog() function
- VU#117394: Buffer Overflow in Core Microsoft Windows DLL

These vulnerabilities all have patches available to prevent exploitation, but because many systems are not properly administered or kept up to date with patches, these old attacks are good enough and continue to work with a high rate of success. Poorly administered systems are also susceptible to malware using techniques such as brute force login attempts against blank or weak user and application passwords.

C. Social engineering

Social engineering involves convincing a user to take an action he or she would not otherwise take. Humans are a weak link in the security chain, and this concept has been exploited by criminals in both the physical and cyber worlds. The following CERT Coordination Center Advisory on social engineering dates from 1991:

CERT®Advisory CA-1991-04 Social Engineering
Original issue date: April 18, 1991
Last revised: September 18, 1997
http://www.cert.org/advisories/CA-1991-04.html

Email, web browser, and instant messaging (IM) applications are some of the more commonly used communications channels for delivering social engineering attacks.

1) Collecting a target list

To develop a target list for these attacks, modern bot malware has the capability to harvest email addresses, IM buddy lists, and other contact information from the compromised system. The malware searches the file system,

[3] Warez (pronounced "wares") refers to illegally distributed copies of licensed software.

registry, PStore,[4] and various address books looking for the information it needs. Once it compiles the contact data, the malware sends the social engineering attack to the targets. When the messages are sent, they can be made to appear as though they are from the friend, coworker, or associate they were harvested from. Due to this, the victim may be more likely to trust the validity of the message and perform whatever action the attacker wants.

2) Email attacks

Email social engineering attacks usually involve prompting the user to open an attachment or follow an unsolicited link. When the file or link is opened, the system becomes directly infected with malware or is subjected to exploits attempting to install malware. These attacks are commonly combined with phishing attempts that attempt to coerce the user into providing sensitive information.

3) Web client attacks

Web client attacks are another technique often coupled with social engineering to spread malware. The victim is lured to malicious web sites, often hosted on other systems under the attacker's control, where multiple exploits may be tried in an attempt to compromise vulnerabilities in the victim's browser or system. If successful, the malware is installed without the user's knowledge. If this automatic and silent compromise technique doesn't work, additional social engineering techniques can be used to convince the user to take whatever actions are necessary to complete the malware install.

A computer user will often make many decisions based on visual cues. An attacker may manipulate a user's course of action by using false visual cues. For instance, if a bogus dialog box is obtrusive and presented in a way that interferes with normal operation of the computer, the user may be coerced into taking an action intended by the attacker that is triggered by accepting or closing the box.

One way attackers leverage this tactic is through the use of pop-ups. Pop-ups can be sent from web pages that are visited, programs that are installed on the machine, and by the built-in Windows Messenger program. These malicious pop-ups tend to state your computer is "infected" and provide an option to download software to clean it up. This software, however, tends to be malware the attackers want to install on the victim's system.

4) Instant messaging attacks

Attacks similar to the ones using email communications are also being applied to harvested IM contacts. In these attacks, IM contacts are sent unsolicited instant messages from the compromised user's IM account. These messages look legitimate but in reality take the user to malicious web sites or begin the download and installation of malicious files. Social engineering attacks utilizing IM have been seen for some time as documented in CERT Coordination Center Incident Note from 1992:

CERT®Incident Note IN-2002-03
Social Engineering Attacks via IRC and Instant Messaging
Release Date: March 19, 2002
http://www.cert.org/incident_notes/IN-2002-03.html

D. Hijacking, purchasing, and trading

Another way to acquire a botnet is through hijacking ("jacking") or stealing it from another attacker. This can be accomplished by using a common feature found in most bot malware, the packet sniffer. Botnet command and control (C&C) communications tend to be unencrypted, and since it's not uncommon for multiple bot infections to be located on the same network or system, attackers commonly instruct their bots to sniff network traffic looking for competing botnet communications. Intercepted C&C communications provide an attacker most of the information needed to locate and "jack" another attacker's botnet.

Botnets are also one of the many things available for sale in the underground economy. The market for botnets is competitive, and they will be sold to anyone willing to pay the asking price ($.04 to $.10 per typical compromised system [2004 Leyden]). If existing bot malware or botnets doesn't meet an attacker's particular needs, custom-designed bot malware and networks can be ordered for a premium.

As with most markets, trading for goods or services is another option. The possibilities are endless, but some of the items commonly bartered for bots include physical goods, such as computers and jewelry, batches of credit card information, shell accounts on servers, or even other botnets.

III. BOT CAPABILITIES

A. Distributed denial of service attacks

Current bot variants commonly include the ability to participate in distributed denial of service (DDoS)[5] attacks against internet targets for revenge or profit. The basic idea behind a DDoS attack is to exhaust some resource required to provide a service, slowing or stopping the ability to process legitimate requests. Some of the more common DDoS capabilities found in modern bot code include PING, UDP, and SYN flooding, as well as application-specific attacks against common internet services such as web and IRC.

1) Flooding attacks

ICMP and UDP flooding attacks target the bandwidth used to provide service. They generally work by sending either a large volume of data that consumes all the bandwidth of a connection or by sending so many packets that the connection,

[4] Windows Protected Store is meant to provide encrypted storage for sensitive data. Some of the data may contain authentication credentials, browser auto-complete information, and digital certificates.

[5] For additional explanation of DoS and DDoS, see "What is a Distributed Denial of Service (DDoS) Attack and What Can I Do About It?" – http://www.cert.org/homeusers/ddos.html.

routers, or servers are overwhelmed processing them and become extremely slow or stop responding.

SYN flooding[6] could be used as a bandwidth consumption attack, but is generally used as an attack against the TCP protocol stack on the target system. Because the client executing the DDoS attack never sends the final ACK packet required to complete the "TCP 3-way Handshake,"[7] the memory used to hold the connection half open is consumed until a timer expires and it is eventually freed. While the amount of memory allocated to this half-open queue can be increased, even if it were set up to handle 10,000 connections, it would require less than 1,200 packets per second to stall the service. With bots capable of sending hundreds of SYN packets per second, the number of bots required to take down a single service is small compared to botnets that often contain thousands of systems.

2) DDoS extortion

DDoS extortion attempts tend to follow a similar pattern, starting with a "sample" attack followed up with an email or other communication threatening a larger DDoS attack if a certain amount of money is not paid. If the extortion attempt is timed with major events, the targeted sites have the potential to loose millions of dollars in revenue and may make the business decision to pay as a form of cash flow risk management. As an added benefit of paying, the attacker may also offer to "protect" the site from other DDoS attacks. Like any protection racket, there are no guarantees. Once the word is out that the site paid, many other attackers may attempt to extort money from it.

B. Exploit scanning/autorooting

Bots commonly include basic port scanners that try to locate open ports on systems. As bot malware has evolved, these basic scanners have been enhanced with advanced exploit scanners and mass autorooter functionality. The sample output shown in Fig. 1 was taken from an rbot variant and is representative of the common format of scanning status update messages seen in bots. It also includes a sample of some of the more commonly targeted vulnerabilities.

<botherder>	.scanstats
<bot12345>	[SCAN]: Exploit Statistics: WebDav: 0, NetBios: 0, NTPass: 0, Dcom135: 0, Dcom445: 0, Dcom1025: 0, Dcom2: 0, MSSQL: 0, Beagle1: 0, Beagle2: 0, MyDoom: 0, lsass: 10, Optix: 0, UPNP: 0, NetDevil: 0, DameWare: 0, Kuang2: 0, Sub7: 0, WKSSVCE: 0, WKSSVCO: 0, Total: 0 in 0d 0h 1m.

Fig.1. Exploit Scanner Statistics.

Bot malware is usually built in a modular fashion. Consequently, as effective exploit code is developed, it can quickly be added to existing scanning/autorooting code, expanding the ways in which the bot can spread. One example of this is the MSRPC exploit[8] that was successfully used in the Blaster worm.

Autorooters are also written to target popular malware backdoors or weaknesses. Fig. 2 on the following page shows a portion of a MyDoom autorooter found in several bots. The spreader logic is executed when the bot's scanner detects the MyDoom backdoor and is representative of the generic techniques used by autorooters to spread bots:

- Stage 1 – connect to the backdoor or vulnerable service
- Stage 2 – exploit vulnerability or authenticate to gain control
- Stage 3 – upload or command the target to download a copy of the bot malware
- Stage 4 – execute the bot malware on the newly compromised system

In the case of MyDoom, the backdoor was inserted by the authors to allow them to upload and execute additional malware. Other malware authors, having learned about this backdoor and how to use it, are taking advantage of the opportunity. Interestingly, once the MyDoom-infected system is infected with the new bot malware, the original MyDoom infection will likely be terminated and cleaned up to prevent others from using the same backdoor.

C. Download and installation

Nearly all bots contain functionality that allows for FTP, TFTP, or HTTP download and execution of binaries. This is the primary method used for updating malicious code in the botnet, but it is not limited to bot updates. It can be used to download any file the attacker commands it to. These files can be launched immediately or at some later time. This ability to download and execute arbitrary programs is often used to install additional malware, such as spyware, adware, or other tools that can be leveraged by the attacker.

D. Click fraud

Click fraud happens when visits are made to an online advertisement, or other resource charged to the sponsor on a per-click basis, by illegitimate means. Bots are commonly used to execute click fraud because they can easily be directed to send web requests that represent "clicks" on the internet ads of certain affiliates. These additional "clicks" boost their affiliate revenues paid by the advertisers. Because the systems infected with bots generally belong to real people and are usually well distributed across the internet, it is very hard to distinguish legitimate clicks from automated bot-generated

[6] CERT® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks – http://www.cert.org/advisories/CA-1996-21.html.

[7] Additional information on TCP 3-way Handshake can be located at: http://www.rfc-editor.org/rfc/rfc793.txt.

[8] VU#568148 - Microsoft Windows RPC vulnerable to buffer overflow - http://www.kb.cert.org/vuls/id/568148.

clicks.

```
...
if(fconnect(sSock, (LPSOCKADDR)&ssin, sizeof(ssin)) != SOCKET_ERROR)   <-- Phase 1: Connects to MyDoom backdoor
{
        if(fsend(sSock, (char*)MyDoomTrailor, 5, 0) == 5) {   <-- Phase 2: sends MyDoomTrailor to provide the "authentication"

                GetModuleFileName(0,botfile,MAX_PATH);   <-- Phase 3: Sends a copy of itself to MyDoom infected machine
                FILE* pFile;
                if((pFile = fopen(botfile, "rb")) == NULL)
                        return FALSE;

                while(!feof(pFile)) {
                        int nRead = fread(szBuffer, 1, sizeof(szBuffer),
pFile);
                        int nSent = fsend(sSock, szBuffer, nRead, 0);

                        if(nRead != nSent) {
                                fclose(pFile);
                                fclosesocket(sSock);
                                fWSACleanup();
                                return FALSE;
                        }
                }
                fclose(pFile);   <-- Phase 4: Disconnects, causing the uploaded bot to execute.
                success = TRUE;   NOTE: No additional action is required to execute the file because the backdoors purpose is to receive a file and execute it.
        }
}
...
```

Fig. 2. MyDoom, a Spreader.

In the example shown in Fig. 3, the `.visit` command directs a single bot to a single URL and makes it look as though it is being referred from the second URL listed. Expanding on this example, an entire botnet could be directed to click on hundreds of target URLs at random intervals generating a steady revenue stream that can be difficult to detect.

Click fraud activity generates large volumes of revenue for attackers and their customers. Estimates have placed click fraud between 5% and 20% of advertising fees paid to search networks [2004 Olsen]. Other estimates have put this number as high as 35% [2005 Penenberg]. According to Olsen's article:

> As a result, U.S. sales from advertiser-paid search results are expected to grow 25 percent this year to $3.2 billion, up from $2.5 billion in 2003, according to research firm eMarketer. From 2002 to 2003, the market rose by 175 percent.

Applying a conservative 10% approach to the figure cited above, click fraud would account for a market loss of $320 million.

```
<botherder>  .visit       http://www.cert.org/
             http://www.referingsite-URL.com/
<bot12345>   site visited.
```

Fig. 3. Click Fraud.

E. Server-class services

To facilitate the operation of botnets, bot malware can include useful services like HTTP and FTP. These types of services allow bots to host:

- phishing sites
- web pages where infected systems can log their infection status
- malware download sites
- spyware data drop off sites
- bot command and control sites

FTP services make bots useful as malware download sites and data drops for spyware and phishing. FTP servers are also popular for the distribution of warez.

Because sending spam is profitable and a good use for bots, an email engine may also be included in the bot malware. These engines accept commands to configure the spam campaign parameters, generally including URLs for the email list and message content. Once the spam job is configured, the bots begin mass mailing until they are told to stop or until they run out of targets. Large-scale spamming can sometimes be detected by monitoring the volume of emails sent from a particular IP or email account in a given time period. This detection method, however, is prone to missing bots used for spamming, especially when the bots are set to rate limit the messages they send or to send messages at random intervals. When there are 10,000 or more bots working to process a mailing list, even 100 messages per bot over the course of a couple hours will result in a million emails being sent with a low likelihood of detection.

Generic backdoor functionality primarily consists of command shells on compromised systems. Attackers use these backdoor shells to connect to the bots for various administrative purposes. In some cases the command shells are not listening for connections, but rather initiate outbound reverse shell connections to a system where the attacker has a listener waiting. The technique of shoveling[9] the shell back to the attacker is done to increase the likelihood of bypassing firewalls or other security devices.

Running these services on bots has several advantages. First, the bots are generally well distributed and utilize the systems of private individuals. This makes them hard to track and shutdown. Second, botnets can consist of thousands of bots, so moving the offered service from one infected system to another is trivial for the bot herder.[10] Third, the resources are free, at least for the attacker. Finally, by using home computers, which rarely have security infrastructure to log and track the activity, the risk of detection and attribution to the attacker is low.

F. Gateway and proxy functions

As mentioned, attackers use infected systems as servers to avoid detection and attribution to themselves. Proxy functionality also supports the evasive activities of attackers. Commonly observed proxy functions include:

- generic port redirection
- HTTP proxy
- Socks proxy
- IRC bounce

1) Generic port redirection

Generic port redirection can cause network connections coming into the bot malware to be sent directly to another system. These can usually redirect any IP based service, including all TCP and UDP requests.

Generic port redirection makes the bots useful as generic bounces through which attackers can hide their true location. For example, attackers can hide their locations as they access IRC servers to control their botnets. If attackers send their connection through a compromised system in the United States, then through one in Russia, then North Korea, and finally connect to the IRC server, tracing them can become nearly impossible. This same technique can be used when spamming, launching phishing attacks, attacking internet facing systems, or any other activity to avoid attribution.

A more specific example of generic redirection is GRE[11] tunneling. Attackers can use this technique to set up virtual circuits across the internet to make traffic flow the way they want as well as to hide the original source. GRE also has the advantage of not being limited to TCP and UDP based protocols. It can encapsulate and deliver almost any sort of packet through the routed tunnel.

2) HTTP and HTTPS proxy

HTTP proxies are a specific kind of proxy used to surf the internet and make it appear as though the attacker is coming from the bot-infected system. To use the infected bot as a proxy, the attacker simply needs to issue commands to start the proxy and set their browser to use the bot's IP address as the proxy server. Any site tracking visitors will now show the bot's IP instead of the attacker's. Some bot's HTTP proxies also include the ability to proxy HTTPS.

3) SOCKS proxy

SOCKS[12] is a protocol that can be used to proxy TCP- and UDP-based services. As is true with most malware proxy functionality, the SOCKS proxy's main purpose is to hide the attacker's true IP address from the remote system being

[9] Shoveling a shell refers to a shell connection where the shell server initiates the network connection calling out to the listening shell client. In effect, the client and server roles are reversed at connection time.

[10] "Bot herder" refers to the attacker that is controlling the collection of compromised systems (bots).

[11] GRE – Generic routing encapsulation is a protocol that can be used to tunnel arbitrary network layer protocols such as IP, IPX, IPSec, ICMP, Appletalk, etc. inside other network layer protocols. It is most commonly used to route non-IP protocols across IP based networks.

[12] SOCKS is defined in RFC1928.

connected to.

Selling or renting SOCKS-capable bots for use in spam distribution is common. Because the bot-infected systems are usually well distributed across many internet-connected systems, the proxies' IP addresses are not likely to be included in spam server blacklists. Even when they are detected and identified as spam proxies, the bots are easy to move, sell, or trade with other bot herders who can use these bots for other functions. These factors are part of what makes the likelihood of tracking, blocking, or shutting down all of the spam relays relatively low.

4) IRC bounce

An IRC bounce is another form of proxy specific to IRC connections. By hiding behind the IP addresses of other people's compromised systems, the attacker achieves a layer of anonymity for activities such as botnet C&C. It also protects against targeted attacks from other attackers. Damage from any DDoS efforts targeted at the attacker simply affects the victim's link while the attacker quickly switches to another compromised system to continue his or her communications with only minor inconvenience.

G. Spyware features

To increase the revenue potential of a bot, spyware features have been engineered into the malware. With these new capabilities, the system is not only valuable for its computing resources and bandwidth, but also for the data belonging to the system's users. Spyware functionality often includes:

- keylogging
- taking screen shots
- browser tracking
- packet capture
- data theft

Armed with spyware, bots can be used to steal valuable personal information and deliver it to attackers for use or sale.

The primary method for retrieving captured data is to automatically upload it to central locations called "drops." These automatic uploads can be triggered by a variety of pre-defined conditions, including elapsed time, quantity of captures taken, data, or any other trigger defined by the malware author. Alternatively, the captures can also be stored on the compromised system and at a later time be retrieved through a backdoor built into the malware.

1) Keylogging

Software key loggers capture keyboard events and record the keystroke data before it is sent to the intended application for processing. This means that even SSL- and VPN-protected applications are vulnerable because the data is capture by the spyware prior to encryption. Keyloggers usually turn their capture on or off based on keywords or events. Some of the more commonly targeted data includes:

- credit card information
- authentication credentials
- personal information useful for identify theft
- email and IM content

Collecting all data related to a computing environment can create a volume of data that is difficult or inefficient to mine for valuable information. Because of this, botnet malware has evolved and now frequently includes features to limit collected data based on environment factors, such as the active process names, active window title, keyword triggers in URLs, web pages, and email content. Focusing the collection parameters and filtering out the noise has helped increase the value of data collected.

2) Screen capture

Much like keylogging, screen captures target data that can be used for financially motivated crimes. When a trigger occurs, such as a keyword appearing in a window or title bar, a screenshot[13] is captured and made available to the attacker. In some cases, this capability has been extended to enabling webcams and microphones on systems to capture audio and video feeds.

3) Packet capture

Packet sniffing capabilities in bots are primarily aimed at two goals. The first is the capture of online credentials, and the second is sniffing information about other botnets. Evidence of this can be seen from source code and binary analysis of bots. The function names and keywords shown in Fig. 4 on the following page were taken from a popular bot.

[13] A screenshot is a picture of the current contents of the screen. It records a picture of what is displayed on the computer monitor at the moment it is taken.

bool IsSuspiciousBot(const char *szBuf) – looks for keywords related to bot activity. Some examples include:

- "JOIN #"
- "302 "
- "366 "
- ":.login"
- ":!login"
- ":!Login"
- ":.Login"
- ":.ident"
- ":!ident"
- ":.hashin"
- ":!hashin"
- ":.secure"
- ":!secure"

bool IsSuspiciousIRC(const char *szBuf) – looks for keywords related to interesting IRC activity. Examples include:

- "OPER "
- "NICK "
- "oper "
- "You are now an IRC Operator"

bool IsSuspiciousFTP(const char *szBuf) – looks for FTP authentication credentials triggered by keywords such as USER and PASS.

bool IsSuspiciousHTTP(const char *szBuf) – may attempt to gather HTTP based authentication credentials and other valuable data. In the case of this sample bot, the keywords appear to target paypal cookies.

- "paypal"
- "PAYPAL"
- "PAYPAL.COM"
- "paypal.com"
- "Set-Cookie: "

bool IsSuspiciousVULN(const char *szBuf) – looks for keywords that indicate vulnerable server versions. Examples include:

- "OpenSSL/0.9.6"
- "Serv-U FTP Server"
- "OpenSSH_2"

Fig. 4. Packet Capture Filters.

Although any keyword could be targeted, the real world examples shown in Fig. 4 are representative of many bots and shed clear light on the general intent of the packet sniffer functions included in the current bot malware.

4) Registry and hard drive searching

Bot malware may include functions that search the system registry and hard drive for items of value. Some of the common items searched for include:

- CD keys
- email addresses
- IM contact information
- clipboard content
- Windows Protected Storage

Some games store their CD keys in the registry or in files on the user's hard disk. If these can be recovered, they can be used directly or sold to those engaged in warez or software pirating activities. Software piracy is big business: "Criminals have been quick to realize the connection with counterfeit products and huge financial rewards." [2000 Cuciz] According to the Cuciz article, worldwide revenue loss on business applications topped $12.2 billion with losses from the video gaming industry approaching almost 109,000 jobs, $4.5 billion in wages, and $1 billion in tax revenue.

Some of the most valuable information useful in spreading malware and for spamming activity includes valid email and IM contact information. A few of the more common techniques for harvesting this information are listed in Fig. 5

- Enumerating the registry for .NET MSN Messenger buddy emails
- Searching for ICQ buddy file location and enumerating the contents
- Searching for the Windows Address Book file and enumerating it's contents
- Searching the hard disk for file that might contain email address data and then parsing those files looking for strings that match email address patterns. Some of the commonly targeted file extensions include:
  - .asp
  - .dhtm
  - .doc
  - .htm
  - .html
  - .inbox
  - .js
  - .msg
  - .php
  - .rtf
  - .txt
  - .vcf
  - .wab
  - .xhtm
  - .xml

Fig. 5. Searching the System.

Microsoft Windows contains a service called the Protected Store. Its purpose is to provide encrypted storage for sensitive data. The following are some examples of data that might be in the PStore:

- Outlook passwords
- passwords for websites
- MSN Explorer passwords
- Internet Explorer AutoComplete passwords
- Internet Explorer AutoComplete fields
- digital certificates

Though the PStore is encrypted, access to it is indirectly controlled by the data owner's login credentials. Since most botnet malware runs under the security context of the user who is logged on, accessing most of this data store is programmatically trivial using the PStore API. Even though the PStore API is largely undocumented by Microsoft, publicly available explanations and source code are available

on the internet to help malware authors with their development efforts.

5) Phishing

As personal information theft has increased, botnet malware has begun to incorporate phishing capabilities. When infected systems are browsing the internet, keywords can trigger the bot to display pre-built fake pages included in the malware or redirect the user to a phishing web site. These pages and web sites display replicas of the original targeted sites and attempt to log and steal personal data.

Attacks sometimes pass the login credentials to the legitimate site or display an error message and then transfer the user to the real site for another login attempt. These techniques are another form of social engineering used to hide the fact that the user has been the victim of a phishing scam.

IV. Command and Control Technologies

A. IRC servers for command and control

The most commonly used C&C server type is internet relay chat (IRC). These servers are favored because they require very minimal effort and administration for use in C&C. Attackers can use public IRC networks or build their own. Private IRC servers can be co-located at "bullet proof"[14] (BP) hosting providers that guarantee uptime, or the software can be installed on one of the compromised systems.

The IRC channel topic can instruct compromised systems within the botnet to perform a specified action. The channel topic shown in Fig. 6 directs the system to perform the following functions:

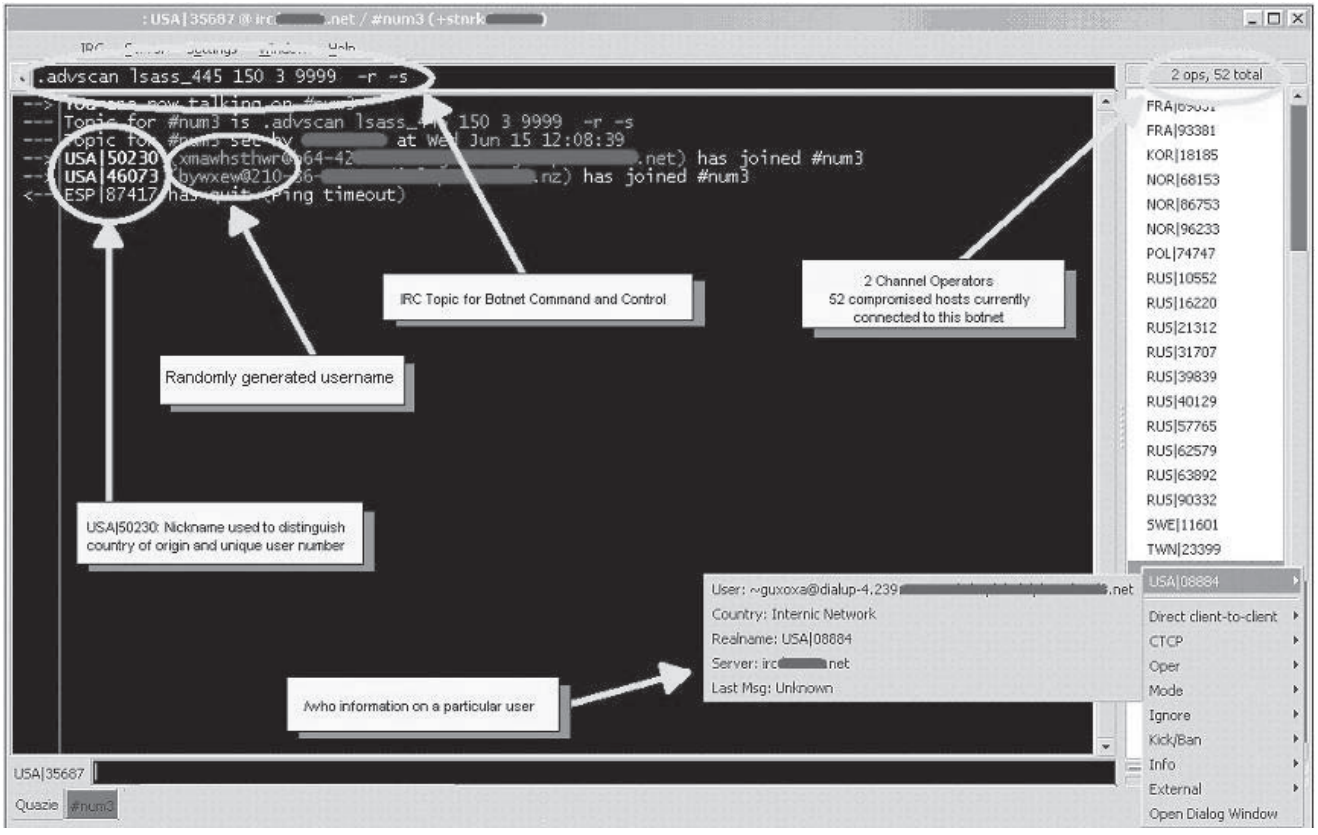


Fig. 6. IRC Command and Control.

[14] The term "bullet proof" hosting implies that the services offered can not be shutdown. These facilities tend to be located overseas or offshore where laws may not be present or as strict.

- `.advscan` – botnet command to scan for vulnerable systems
- `lsass_445` – attempt to exploit vulnerable hosts using VU#753212
- `150` – the number of concurrent threads
- `3` – the number of seconds to delay between scans
- `9999` – specified amount of time to perform the scanning activity
- `-r` – the IP addresses it attempts to scan should be generated randomly
- `-s` – the scan should be silent and not report its findings back in the channel

B. *Web-based command and control*

Another method attackers use to control a botnet is HTTP. Attackers most commonly configure bot malware to instruct the compromised system to access a PHP script on a web site with its system-identifying information embedded in the URL. A web interface can be created to track and control the botnet. Attackers use the interface to send commands to an individual system or to the entire botnet via the HTTP responses. A more covert way for the malware to receive its commands is for it to query a web site under the attacker's control. The malware knows what information to expect and how to interpret it into valid commands.

Upon infection, the compromised system attempts to contact the web-based C&C server and notify it of the machine's IP address, what port its proxy is running on and its machine identification string, which can be used to identify and communicate with individual bots. Samples of this information are shown in Fig 7.

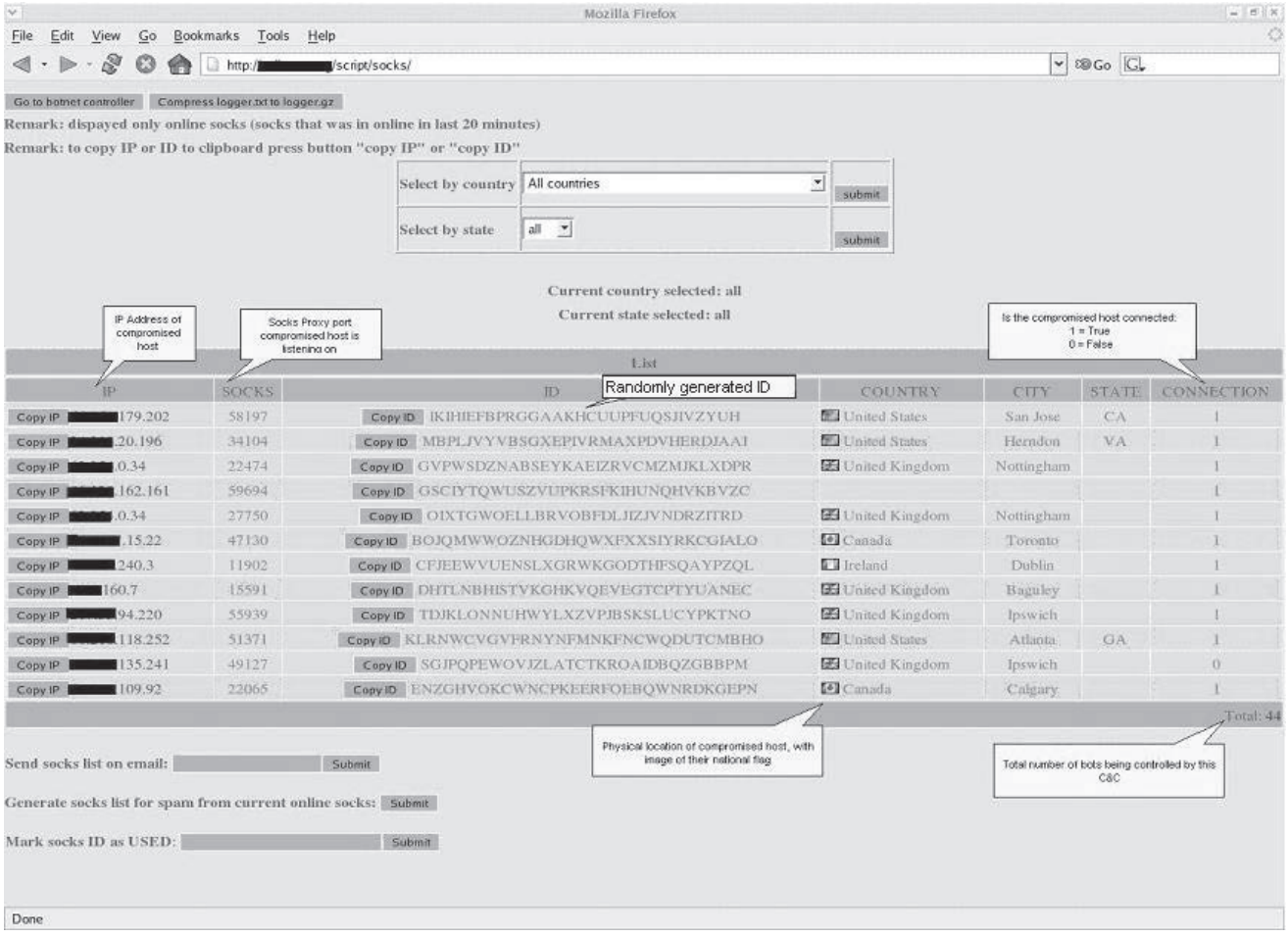


Fig. 7. Web-based Command and Control, Reporting Interface.

Fig. 7 and 9 present web-based C&C interface views.

```
GET
/script/logger.php?p=45324&machineid=SOJXXHNSAKNTUB
VWQBGYBBXAQKIHMPU&connection=1&iplan= HTTP/1.1
Host: WebBased-C&C-domain-name.com
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Fri, 01 Jul 2005 15:22:06 GMT
Server: Apache/1.3.31 (Unix)
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html
```

Fig 8. Sample HTTP Logging of Infection.

The cmd.php page shown in is an example of a web page used by bot herders to send commands to compromised systems within the botnet. These commands are entered into the page and, upon submission, a command file is created (cmd.txt). The compromised systems query for the cmd.txt file every 5 seconds and then perform any of the commands issued to them. Some of these commands direct bots to:

- download and execute files from a URL
- execute shell commands
- adjust the storage location of screen captures and URL logs
- adjust the hosts file on the compromised system

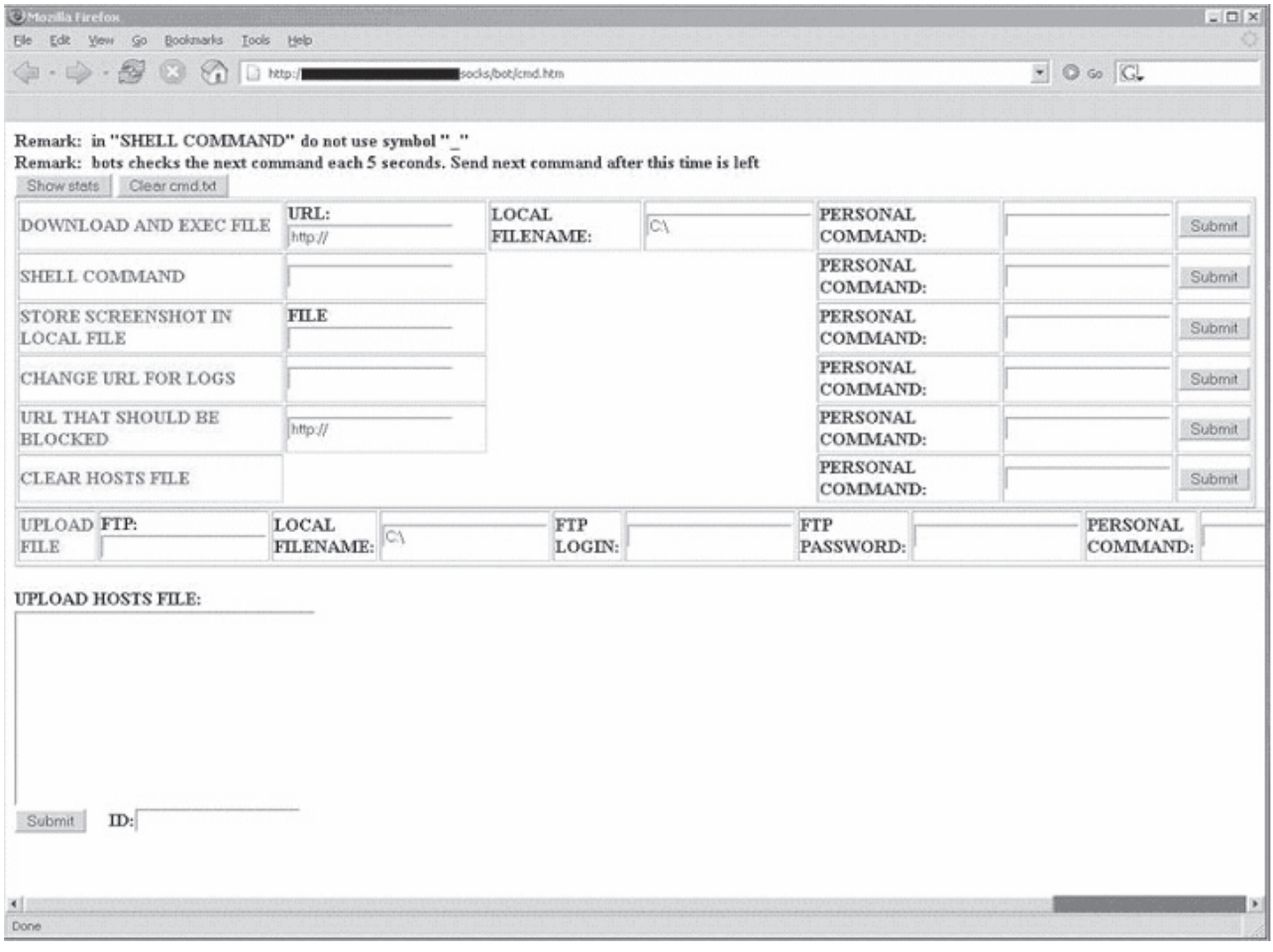


Fig. 9. Web-based Command and Control, Command Interface.

C. P2P command and control

Peer–to-peer (P2P) is another C&C architecture used by the attacker community to control botnets. The key feature of P2P as a command and control structure is that it has no real central server that can be shutdown to disable the botnet. Two of the more established pieces of botnet malware that have implemented this C&C structure include Phatbot[15] and Sinit.[16]

Phatbot utilizes the Gnutella cache servers to establish its list of seed peers. The P2P protocol used on the compromised systems is a modified version of the WASTE[17] protocol. Sinit establishes its list of peers by randomly sending out packets and utilizes digitally signed code to ensure only specified files are executed.

D. DNS command and control

While the command and control architectures listed above are the most prevalent, the attacker community will continue to adapt and look for new botnet communication channels. Dan Kaminsky demonstrated he could broadcast streaming radio over a covert channel located in DNS [2004 Lemos]. Another example that has been observed was a piece of malware that constructed a DNS-style name using a hard-coded domain name, which it then attempted to resolve using the gethostbyname() API. The DNS server authoritative for the queried domain responded with an answer that contained encoded information for the system. This made the C&C traffic look like legitimate DNS resolution traffic. The biggest advantage to using DNS as a C&C mechanism is that DNS is used by everyone and is permitted through the majority of firewalls. Even when a localized DNS server is used and DNS queries are blocked by the firewall, the local DNS sever could still forward queries to the authoritative server and the C&C traffic would still pass through the firewall.

V. Defending the Botnet

A. Preserving availability via DNS

To maintain C&C server availability and prevent complete shutdown, attackers configure the malware to connect to a fully qualified domain name (FQDN) rather than an IP address. If an attacker uses an IP address, and that IP address is removed from the internet (routed to a blackhole or physically shutdown), the attacker will loose all control of his or her botnet. If an FQDN is used, both the IP address(s) and the FQDN would need to be removed before the attacker would loose total control of the botnet.

Attackers will either buy an FQDN (usually with a stolen credit card) or use one provided by dynamic DNS providers. Some dynamic DNS providers also offer free sub-domains. By utilizing multiple sub-domains, the attackers are able to hide their malicious activities. Some of these activities include load balancing requests, creating staging areas and implementing relays. Another advantage to using dynamic DNS providers is that they set their TTL value on their domains relatively low (five minutes or less), which means changes made to an FQDN take effect almost immediately with very minimal downtime. The attacker's abuse of dynamic DNS providers has given them greater flexibility in how they avoid detection and shutdown of their infrastructure.

B. Authentication

Bot herders often employ password authentication in their bots to keep unauthorized users from controlling them. In the malware binaries, the password is sometimes stored in clear text, but increasingly, methods have been devised to prevent analysis and disclosure to would-be "jackers" and those in the IT security community. A common technique for protecting the password involves keeping it encoded, then encoding the password the user supplies just before the compare. A similar technique is to use a checksum value to represent the password and to calculate a checksum on the supplied password for comparison.

Other forms of authentication include:

- IRC server and channel passwords
- verifying the username or domain of the would-be controller
- verifying IRC server name

C. Modifying the command language

Stealing botnets requires some knowledge about how to control the bots being stolen. Because a lot of bot code is reused, the commands and authentication mechanisms are becoming widely known. Additionally, there are well known bot communication signatures coded into intrusion detection systems (IDS), intrusion prevention systems (IPS), and other bots' packet capture filters that look for known bot commands. These are just a few of the reasons that some attackers modify the command and control language used by their bots.

For example, attackers commonly change the login command. In rbot, the default login command is `login`, an attacker could easily change this to `nigol`[18], or something more obscure, raising the barriers to detection and control. Other command names can be modified just as easily so even if a competitor acquired the passwords, he or she would still need detailed knowledge or packet captures of command sequences to control the botnet.

D. Customized IRC daemons

Like bot code, IRC daemons (IRCd) are publicly available and reused amongst the attacker community. Attackers can use out of the box configurations or customize the IRCd to meet their needs. Some commonly observed modifications include performance customizations that optimize them for

[15] Technical analysis can be located at: http://www.lurhq.com/phatbot.html.
[16] Technical analysis can be located at: http://www.lurhq.com/sinit.html.
[17] Additional information regarding WASTE can be located at: http://waste.sourceforge.net/.

[18] nigol – login typed backwards

running botnets by stripping out the overhead functionality necessary to run legitimate, full-service IRC networks. Other observed modifications that focus on secrecy and protecting the botnet include:

- removing the `/who`, `/list`, and `/stats` commands
- adding alerts to the operator in the channel when any of the above commands are attempted
- hard coding the IRCd to report a low number of users, even though thousands may exist
- setting default channel modes to include: `+i`, `+p`, `+s`, `+t`[19]

E. SSL

If clear-text bot communications are captured, the data may reveal the bot authentication information and commands used to control the bot. Rivals can use this information to take control of the bots, and IT security personnel can use it to remove them from infected systems. Consequently, some attackers implement SSL encryption to protect the communications between the bot and the command and control system. Although SSL-enabled bots have been observed in the wild, it is still a relatively rare protection mechanism due to the overhead involved in implementation and because many public IRC servers do not support SSL-encryption. Another reason SSL is not widely used is because it has not been a necessary feature to maintain a profitable botnet. If traffic capture begins to cut too deeply into profits, there is no doubt the use of network encryption will begin to rise.

F. Securing the system

After a bot is installed on a system, the attacker will want to secure it and remove other malware to keep others from stealing their newfound system and also to make sure system performance is not degraded by other running malware. To do this, some bot variants take steps to secure vulnerabilities in the system such as disabling DCOM or network shares.

A common technique for removing competing malware is to search for processes, registry entries, and files related to known malware and then try to disable or remove them from the system. The code in Fig. 10 presents an example of this functionality.

Malware starts a thread that executes the infinite loop in ExecutableKill function listed below:

```
const char *FilenamesToKill[18] = {
        // W32.Blaster.Worm
        "msblast.exe",
        "tftpd.exe",
        // W32.Blaster.B.Worm
        "penis32.exe",
        // W32.Blaster.C.Worm
        "index.exe",
        "root32.exe",
        "teekids.exe",
        // W32.Blaster.D.Worm
        "mspatch.exe",
        // W32.Blaster.E.Worm
        "mslaugh.exe",
        // W32.Blaster.F.Worm
        "enbiei.exe",
        // Backdoor.IRC.Cirebot
        "worm.exe",
        "lolx.exe",
        "dcomx.exe",
        "rpc.exe",
        "rpctest.exe",
        // common trojan filenames
        "scvhost.exe",
        "bot.exe",
        NULL
    };

Pseudo Code to represent ExecutableKill
{
Infinite_loop {
    for each process in running process {
        if process in FilenamesToKill array {
            terminate the process
            delete the file associated with the process
        }
    }
    pause for 1.5 seconds
} // restart loop (infinite_loop)
```

Fig. 10. Terminate Competing Malware.

The code in Fig. 10 represents functionality found in an sdbot derivative, but very similar code is present in most bots, as well as other types of malware. The list of malicious program files is easily modified as new threats become more widespread or threaten the bot herders "asset." When this code is executed, it terminates any running processes having the names listed and attempts to delete the files associated with those processes. In this particular instance, the code continues to monitor for new instances of malware, checking for new processes every 1.5 seconds.

Many of the techniques used to secure the system can be used in reverse when the bots are commanded to remove themselves. This means that even after the bot malware is removed, the system can be left with open vulnerabilities that need to be secured to prevent future infections. Fig. 11 shows sample code from a bot that un-secures the system as it is

[19] IRC option meanings:
+i – sets the channel to only accept requests to join from invited clients
+p – attempts to keep the channel secret by not showing it in /WHO, /NAMES or /LIST listings
+s – attempts to keep the channel secret by not showing it in /WHO, /NAMES or /LIST listings
+t – only channel ops my change the topic

```
#ifdef WIN32
                /// should unsecure system as remove bot to allow recycling //

                // Set EnableDCOM to "Y"
                HKEY hkey=NULL; DWORD dwSize=128; char szDataBuf[128];
                strcpy(szDataBuf, "Y"); dwSize=strlen(szDataBuf);
                LONG lRet=RegOpenKeyEx(HKEY_LOCAL_MACHINE, "Software\\Microsoft\\OLE", 0,
KEY_READ, &hkey);
                RegSetValueEx(hkey, "EnableDCOM", NULL, REG_SZ, (unsigned char*)szDataBuf,
dwSize);
                RegCloseKey(hkey);

                // UnSecure Shares
                Execute("net.exe", "net share c$=c:\\");
                Execute("net.exe", "net share d$=d:\\");
                Execute("net.exe", "net share e$=e:\\");
                Execute("net.exe", "net share ipc$");
                Execute("net.exe", "net share admin$");

                // Delete Autostart
                if(g_pMainCtrl->m_cBot.as_enabled.bValue)
                        g_pMainCtrl->m_cInstaller.RegStartDel(g_pMainCtrl-
>m_cBot.as_valname.sValue);
                if(g_pMainCtrl->m_cBot.as_service.bValue)
                        ServiceDel(g_pMainCtrl->m_cBot.as_service_name.sValue);
#endif
```

Fig. 11. Un-securing the System on Bot Removal

removing itself. The comment in the source code is "`/// should unsecure system as remove bot to allow recycling //`", a clear indication that this is done to make future infections more likely.

G. Disabling security applications and updates

Bot malware includes functionality to disable a number of security mechanisms. Commonly targeted security applications include Windows XP built-in firewall and its anti-spyware technology, other manufacturer's anti-spyware tools, anti-virus applications, and security or management tools that may be used to detect, kill, or remove the bot malware from the system.

There are many ways to terminate or block access to these applications, but the most common approach includes walking the list of running processes, comparing them against a static list of process names known to be associated with the application types listed above, and terminating any matching processes. This is a simple technique, but it is still very effective. This process is similar to the method shown in Fig. 10 used to terminate competing malware that might be installed on the system.

Disabling security updates can be done by blocking access to internet sites that the applications use for downloading updates and new signatures. Since the security software may require these updates to detect new malware, this may prevent tools like anti-virus from detecting the particular version of the bot the system is infected with even after a signature has been developed. A commonly used technique to cut off the application from its update site is modifying the user's hosts file, inserting entries for the update site's domain names that point to 127.0.0.1[20] or to some other address of the attackers choosing. This keeps the IP address from properly resolving and effectively blocks the software from connecting and downloading updates. On Windows XP systems, the hosts file is stored in C:\Windows\System32\drivers\etc. Looking at this file for unusual entries may reveal information about whether a system is infected.

Attackers can also create another hosts file in a separate location and then modify the system registry to make the

[20] 127.0.0.1 is commonly referred to as the loopback address and is used to represent "this" host. Traffic sent to it will be routed to the local system and does not generally reach the internet or other network hosts.

system use the new hosts file instead. This is useful because it hides the modifications from most users that would not know to look for an alternate hosts file location.

H. Binary obfuscation

Binary obfuscation includes techniques like packing[21] the executable to make it difficult to reverse engineer or to pull valuable strings data from a captured bot binary. Some other forms of obfuscation commonly encountered involve encoding the strings used by the binary, such as passwords, C&C information, commands, etc. The bot code then executes a decode function just before the malware needs the obfuscated data, or it encodes the received data and then compares it to the encoded data. Attackers do this to prevent others from locating C&C information, authentication information, or other traffic that could be used to steal the bots from their herder.

Attackers are aware that some of this data can be recovered through runtime analysis, such as sniffing the network connection. To prevent revealing all of their secrets, bots can be coded to use a primary password or primary C&C system, but also have a secondary C&C network that only activates after a period of time has passed or if the primary is made unavailable. In this way, quick runtime techniques may only reveal the initial connection information but will leave the details of the backup network unknown.

Additional items commonly protected through obfuscation include a backdoor password that can be used by the original bot author to take over the bots. There are several precompiled bots that use configuration programs to set up the C&C architecture and authentication information. If the attacker configuring the bot doesn't have source code, he or she may be unable to see the backdoor passwords that will enable the original malware author to take over or "borrow" the bots.

These examples and others have been observed in the wild and utilize obfuscation to prevent or delay detection of their hidden functionality.

I. Rootkit and anti-analysis techniques

Recently, there appears to be an increase in the use of rootkit and anti-analysis technology in bot malware. In some recently analyzed bot malware, one of the initially called functions executed instructions equivalent to code shown in Fig. 12 does a simple check to see if SoftICE is loaded by attempting to open a handle to its driver. If successful, it knows that debugger is present. In addition to this check, the function in which this code was found also performed other checks for debuggers as well as tests to see if the binary was running in a virtual machine environment. If any of these conditions were detected, the malware terminated itself so further runtime analysis could not be completed.

```
hFile = CreateFile("\\\\.\\NTICE",                    <-- Attempt to open a handle to SoftICE driver
                   GENERIC_READ | GENERIC_WRITE,
                   FILE_SHARE_READ | FILE_SHARE_WRITE,
                   NULL,
                   OPEN_EXISTING,
                   FILE_ATTRIBUTE_NORMAL,
                   NULL);

if( hFile != INVALID_HANDLE_VALUE )                   <-- If successful, return TRUE to indicate SoftICE is running
  {
    CloseHandle(hFile);
    return TRUE;
  }

return FALSE;
```

Fig. 12. Debugger Detection.

[21] In the context of malware, packing generally refers to compressing or obfuscating a file so that it can not be directly analyzed without first unpacking the file.

Other bot malware has been packaged with popular rootkits such as "hacker defender." These rootkits attempt to hide the bot malware from security tools and other utilities that might reveal its existence and activity.

Expending increased effort to incorporate new and more advanced techniques is a clear indication of the changing competitive environment. Attackers are very good at doing just enough to make profits from their activity. If advanced techniques are becoming more common, they are likely not being born out of curiosity, but rather as a result of market forces.

VI. Tracking botnets and bot herders

A. *Analysis of malware and network traffic*

One of the easiest and quickest ways to obtain botnet information is to perform runtime analysis on a piece of malicious code. Performing runtime analysis can be as simple as running a packet capture on an isolated machine. As the infection process occurs, network traffic will be generated as the infected system attempts to log into the botnet. This kind of captured information can include the FQDN for the C&C server, the channel name and password, and usually a randomly generated nickname.

A more in-depth and time consuming approach is to reverse engineer the malicious executable. Reverse engineering analysis can reveal similar information to runtime analysis, as well as other details including hidden functions, passwords, and details that might not immediately show themselves at runtime. Reverse engineering analysis can require a great amount of time and skill, but when the work is complete there are no secrets about the malware functionality left unrevealed.

Reviewing network traffic, router, IDS, and firewall logs may also reveal a botnet on the network. Placing a packet sniffer at a location that will permit the viewing of all ingress/egress traffic will reveal much of the same information.

In an attempt to hide their tracks, attackers relay or bounce through systems in their botnet, or from other locations. Frequently, the network relays cross economic and geographic boundaries, making it extremely difficult to trace attackers back to their origin or to get international cooperation with the investigation. The attacker community knows this is the case and uses it to their advantage.

Even when cooperation can be obtained for an investigation, differences in laws, language, politics, and priorities between countries make prosecution difficult. The activities themselves may be overlooked for a variety of reasons, including insufficient staffing, differing perceptions of severity, low impact in a given region, bribery, extortion, and fear.

B. *Attribution through code*

Attribution can be a difficult task. Source code attribution provides a good example of this difficulty. Anyone can write or modify code, put it on the internet, and place anyone's name on it. Often we see source code commented about where it was taken from or who may have written it, but attempting to determine the accuracy of that information can be difficult and time consuming. While many attackers may not have the capabilities to write malicious programs, for a price, programmers are readily available to create malware that meets their needs.

Attackers or crews that have programming capabilities tend to co-develop and share code, making it difficult to pin the efforts down to one person. One may even have problems pointing to a specific crew, since code maybe shared among crews or published on the public internet for anyone to download and distribute. In July of 2004, the author of the Bagle virus released a copy of the virus with the source code. While the exact reason is unknown, the release of the source code is making it easier for anyone to create more versions or tailor it to their specific needs without having to write it from scratch.

C. *Follow the money trail*

As shown throughout this paper, much of the functionality and activities of the attacker community are driven by the desire for financial gain. The ultimate goal of the attackers is to use their ill-gotten information and capacity to generate cash in the physical world. Examples of this include deposits from DDoS extortion, payments from spamming, cashing out bank accounts and credit cards, purchasing goods with stolen credit card information, identity theft, and the sale of fake identification documents. As the money generated from these activities is transferred between accounts, moved through cashiers, and ultimately ends up in the hands of the attackers, Law Enforcement may be able to follow the money trail and locate the attackers responsible.

References

Extortion via DDoS on the rise
Denise Pappalardo and Ellen Messmer
MAY 16, 2005
http://www.computerworld.com/networkingtopics/networking/story/0,10801,101761,00.html

The Bandwidth Report
June 21, 2005
http://websiteoptimization.com/bw/

Phatbot arrest throws open trade in zombie PCs
John Leyden
May 12, 2004
http://www.theregister.co.uk/2004/05/12/phatbot_zombie_trade/

Exposing click fraud
Stefanie Olsen
July 19, 2004
http://news.com.com/Exposing+click+fraud/2100-1024_3-5273078.html

BlowSearch Tackles Click Fraud
Adam L. Penenberg
June 16, 2005
http://www.wired.com/news/culture/0,1284,67873,00.html?tw=wn_5culthead

Software Piracy Report:
David Cuciz
June 2000
http://archive.gamespy.com/legacy/articles/spr1_a.shtm

Internet's 'white pages' allow data attacks
Robert Lemos
July 31, 2004
http://www.defcon.org/html/links/dc_press/archives/12/news_dnshack.htm

Operation Firewall:
United States Secret Service
October 28, 2004
http://www.secretservice.gov/press/pub2304.pdf

VU#568148 - Microsoft Windows RPC vulnerable to buffer overflow
http://www.kb.cert.org/vuls/id/568148

VU#753212: Microsoft LSA Service contains buffer overflow in DsRolepInitializeLog() function
http://www.kb.cert.org/vuls/id/753212

VU#117394: Buffer Overflow in Core Microsoft Windows DLL
http://www.kb.cert.org/vuls/id/117394

CA-1991-04: CERT®Advisory CA-1991-04 Social Engineering
Original issue date: April 18, 1991
Last revised: September 18, 1997
http://www.cert.org/advisories/CA-1991-04.html

CERT®Incident Note IN-2002-03
Social Engineering Attacks via IRC and Instant Messaging
Release Date: March 19, 2002
http://www.cert.org/incident_notes/IN-2002-03.html

Uma Arquitetura de Controle Inteligente para Robôs Foreses

José Helano Matos Nogueira, *Perito Criminal Federal, Diretoria Técnico-Científica, Departamento de Polícia Federal, SAIS, Quadra 07, Lote 23, Brasília-DF, Brazil*

***Abstract*—For some time now it has been argued new forms to create efficient control architecture for mobile robots. This work presents a new architecture to creating intelligent mobile robots, called forensic robots which interact with uncertain and dynamic environments as crime scene. To demonstrate the real functionality of this architecture it was created a conceptual model of forensic robot (ROFO). ROFO is divided in modules that they are inspired by the anatomy and physiology of the human beings. In addition, it uses advanced artificial intelligent techniques and neural networks to generating its capabilities of planning, control, and reactive behavior.**

***Palvras-Chave*—ciência forense, informática forense, inteligência artificial, robótica.**

I. Introdução

O projeto de arquiteturas de controle para robôs que executam tarefas em ambientes especificados tem sido um tópico de interesse em robótica, inteligência artificial e pesquisas de tecnologias aplicadas nos últimos anos [1]-[3], [8],[7]. Todavia, tem se verificado que grande parte das arquiteturas propostas exibem somente uma forma bastante limitada de comportamento inteligente do robô em relação ao seu domínio de atuação. Isto se comprova principalmente devido a falta de uma metodologia apropriada para interação do robô com seu ambiente, destacadamente na descoberta de vestígios em locais de crime, onde o uso de módulos de estruturas de controle de robôs tradicionais são bem distantes da realidade prática. A idéia central deste trabalho é propor uma arquitetura de controle inteligente para uma nova geração de robôs que possa auxiliar os peritos criminais em suas tarefas diárias de investigação e busca de vestígios em ambientes quase sempre desconhecidos e muitas vezes inóspitos, tais como locais pós-explosão, laboratórios clandestinos e ambientes saturados de materiais tóxicos ou radioativos. A esta nova geração de robôs que utiliza uma arquitetura baseada em planejamento computacional, redes neurais, reconhecimento de padrão e técnicas avançadas de inteligência artificial aplicada no campo de atuação judicial será chamada a partir deste ponto de robôs forenses.

Para tratar as limitações impostas pelas tecnologias anteriores, este trabalho cria uma nova arquitetura de controle genérica para criação de robôs forenses inteligentes e móveis que interagem com ambientes externos incertos, insalubres, perigosos e dinâmicos, campo de vasta aplicação na área pericial. Esta arquitetura é inspirada na anatomia e fisiologia do modelo biológico dos seres humanos, mais especificamente em seu sistema nervoso central. Para tanto, a metodologia de comportamento utilizada está baseada em técnicas de inteligência artificial que são responsáveis pela representação do conhecimento, pelo reconhecimento de padrões, pelo planejamento e pela reatividade nestes tipos de robôs. Já as estruturas de controle da arquitetura estão divididas em módulos que buscam um comportamento mais realista e inteligente para os robôs forenses.

Com o intuito de demonstrar a funcionalidade desta arquitetura de controle foi criado o modelo conceitual de um RObô FOrense (ROFO) que interage de forma dinâmica com ambientes complexos e não estruturados.

II. Modelo Biológico Representativo

Para que se tenha uma arquitetura completa para um robô móvel aplicado em locais de crime torna-se necessário um modelo que seja eficiente e ao mesmo tempo inteligente. Portanto, nada mais natural do que usar como analogia de controle o modelo biológico dos seres humanos.

No ser humano todo o controle de suas atividades vitais é realizado por seu sistema nervoso. O sistema nervoso do ser humano é uma rede entrelaçada extensa que consiste de duas partes: periférica e central. Para o propósito deste trabalho, a pesquisa será concentrada no Sistema Nervoso Central (SNC), em seus dois componentes: a medula espinal e o encéfalo (cérebro, cerebelo e bulbo) [4]. A figura 1 apresenta a anatomia básica do SNC do ser humano, o mais sofisticado sistema nervoso dos seres vivos.

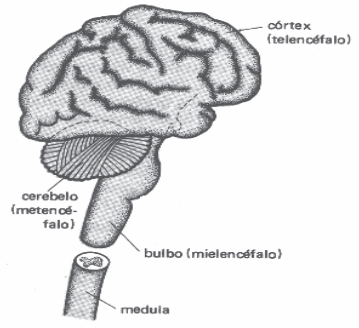


Fig. 1. O sistema nervoso central humano.

III. Arquitetura de Controle para Robôs Forenses

A arquitetura de controle que foi projetada é uma arquitetura genérica que pode ser aplicada a uma ampla variedade de robôs móveis. Todavia, para facilitar a demonstração das estruturas de controle, torna-se útil considerar todas elas em um único robô, complexo o bastante para deixar evidente a necessidade de cada mecanismo, mas simples o suficiente para fornecer um bom acompanhamento do funcionamento da arquitetura. Portanto, será apresentado como exemplo de aplicação da arquitetura o RObô FOrense (ROFO) que requer ambas capacidades de planejamento e reatividade.

Assim como no SNC humano a arquitetura de controle do ROFO está dividida em duas grandes porções: o encéfalo (córtex cerebral, cerebelo e bulbo) e a medula espinal. No córtex cerebral o ROFO realizará o controle das atividades de planejamento (geração e reconhecimento de planos), o reconhecimento de padrões, reatividade e a agenda de execução das ações. Para a geração de planos já se encontra implementado um Gerador de Planos (PIT), que fornece uma nova metodologia para geração automática de planos — a estratégia de meios-fins combinada com a regressão de metas [10], [9]. Desta forma o PIT consegue contornar o *frame problem* [5] e ainda gerar planos otimizados. Também encontra-se implementado o módulo de reconhecimento de planos, criando um novo paradigma, chamado Sistema Reconhecedor de Planos (SRP), formalmente descrito em lógica clássica de primeira e segunda-ordem, no item B da seção IV. A grande vantagem do uso do SRP incorporado ao ROFO é que ele reconhecerá as ações e planos de objetos e agentes externos antes de executar qualquer procedimento reativo de alto impacto.

Na parte referente ao reconhecimento de padrões será implementada a abordagem conexionista de redes neurais acoplada ao módulo de coordenação sensora. Para realização da reatividade será utilizado um Sistema Módulo Reativo (SMR) que se encarregará das ações condicionais reativas. Para a representação do conhecimento e execução das tarefas será utilizada a técnica de agenda de execução [3] que receberá as ordens de execução do SMR. O cerebelo do ROFO será o responsável pela coordenação motora que utilizará como estratégia de navegação o algoritmo de busca heurística em tempo real - RTA*, trabalhado em [10]. No bulbo ficará centralizada a coordenação sensora que interagirá com a rede neural de reconhecimento de padrões. No módulo da medula espinal ficarão distribuídos os geradores de movimentos e os filtros sensores.

Portanto, o ROFO é um robô autônomo abstrato que executará a navegação e a manipulação externa por longos períodos de tempo. O ambiente de trabalho do ROFO é qualquer ambiente externo não estruturado como movimentações em locais onde há ameaça de bombas deixadas por criminosos ou terroristas, locais pós-explosão, locais de difícil acesso. Ou seja, aplicar esta nova categoria de robôs forenses em locais perigosos ou insalubres (tóxicos, inflamável, radioativo, corrosivo, dentre outros) ou que não seja possível a atuação do perito humano. O comportamento do ROFO está dividido em camadas: superior e inferior. A camada superior está responsável pela visão e percepção. É nesta camada que o robô identifica os objetos externos e seus respectivos movimentos através do uso de reconhecimento de padrões e de planos. Já a camada inferior está responsável pela realização de ações. Estas ações consistem basicamente na navegação entre os ambientes externos, na geração de planos para atingir os seus objetivos e na reatividade. Cada estado do robô é representado através do modelo de quadro-negro [6]. Este modelo será utilizado em conjunto com a estrutura de representação do conhecimento baseada em agenda de execução, que por sua vez representará os planos, tarefas e ações.

A estrutura de decisão do ROFO é dividida em duas porções principais: planejar e agir. O planejamento é garantido pelo Gerador de Planos (PIT) que efetiva o planejamento inteligente de tarefas. As ações, por sua vez, são executadas com base no sistema Reconhecimento de Planos (SRP) e no Sistema Módulo Reativo (SMR). O controle do ROFO está, basicamente, em seu córtex cerebral, de forma semelhante a arquitetura apresentada na fig 2.

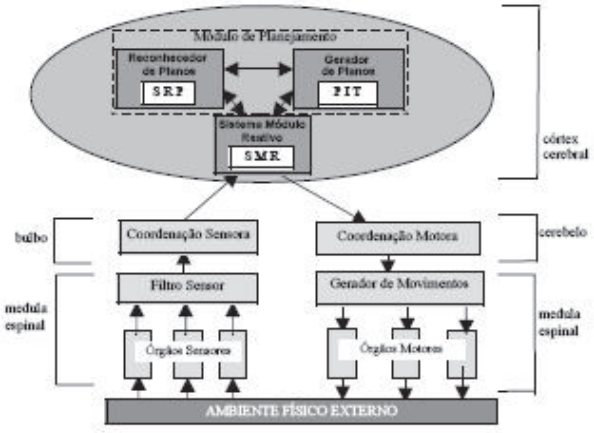


Fig. 2. Arquitetura de controle para robôs forenses

IV. Módulo de Planejamento

Com o objetivo de apresentar a realidade prática do módulo de planejamento da arquitetura de controle em robôs móveis, serão apresentados a seguir a geração e o reconhecimento de planos incorporados ao ROFO.

A. Gerador de Planos

Um *plano* é formado por um conjunto de ações que serão executadas pelo ROFO. O processo de *geração de planos* de forma automática consiste em dividir a tarefa a ser executada em uma seqüência de passos que soluciona o problema modelado. No módulo Gerador de Plano (PIT) do ROFO, se um caminho improdutivo é detectado, então um novo caminho pode ser explorado, retrocedendo-se até o ponto da última escolha. O PIT utiliza como entrada um conjunto de operadores (Op_i) e um problema. O problema é caracterizado por um estado inicial (E_i) e um estado final (E_f) que representa os objetivos. Além disso, deve haver outros dados sobre o domínio de aplicação que são armazenados em uma base de dados. A base de dados é uma estrutura composta de fatos e

regras que mapeiam o conhecimento de determinado domínio de aplicação em um modelo computacional. O plano resultante é fornecido ao Sistema Módulo Reativo (SMR) que se encarrega da execução do plano. Vide figura 3.

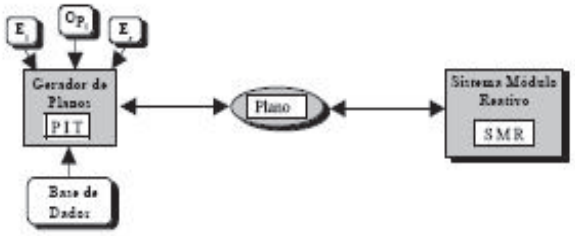


Fig. 3. Geração de planos e sua execução no ROFO

A estratégia de busca de soluções utilizada na geração de planos do ROFO será a estratégia de *meios-fins* [6]. A inclusão desta estratégia de raciocínio para robôs móveis deve-se ao fato dela permitir a divisão do problema em subproblemas menores e então solucionar primeiro as partes mais importantes para só depois solucionar as partes menos relevantes. Isto é efetuado através da seleção de operadores que correspondem as ações a serem realizadas pelo robô. A outra técnica utilizada em conjunto com a estratégia de meios-fins é a *regressão de metas* [10], [9]. A idéia da regressão de metas é que o planejador deve preservar os objetivos que já foram atingidos (satisfeitos) em etapas anteriores no processo de geração de planos. Portanto, planejadores sem regressão são incompletos. A solução utilizada no PIT para se obter a completude é garantir que planos ótimos sejam gerados e isto só é possível permitindo-se a interação entre os objetivos através da regressão de metas.

B. Reconhecedor de Planos

Um problema não tratado nas arquiteturas de controle encontradas na literatura de robótica e inteligência artificial é o reconhecimento de planos, pois o robô está sempre gerando planos e/ou reagindo. Todavia, existem situações em que torna-se necessário primeiro que o robô reconheça a intenção do agente externo para só depois reagir ou executar um novo planejamento. Portanto, este trabalho apresenta uma nova técnica de reconhecimento de planos elaborada especificamente para o uso em robôs móveis. Esta técnica foi criada a partir da teoria formal genérica encontrada em [9]. O *processo de reconhecimento de planos* consiste em encontrar o plano que contenha a representação das ações ou movimentações de um agente externo. Uma vez encontrado o plano este é montado em um modelo que será utilizado para construção de um novo plano que será utilizado como resposta ao plano do agente externo, ou este novo plano é enviado diretamente ao SMR do ROFO para que seja efetivado alguma reação, de acordo com as figuras 2 e 3.

Para efetuar o reconhecimento de planos foi criada uma Técnica Formal de Reconhecimento de Planos (TeFoRP) que está baseada em lógica clássica de primeira e segunda ordem. Neste momento vale a pena destacar o fato de que a TeFoRP possui uma nova formulação adaptada exclusivamente para o reconhecimento dos planos de agentes externos. Assim, a TeFoRP foi projetada com a finalidade de prover funcionalidade aplicada a qualquer robô móvel de uma maneira simples e ao mesmo tempo robusta. Visando a formalização e a corretude da TeFoRP algumas definições básicas tornam-se necessárias neste momento.

DEFINIÇÃO 1 (EVENTO)

Um evento $E_i(x)$ é um predicado unário que representa *ações* e *planos* realizados pelo agente x (x pode ser o ROFO ou um agente externo). O conjunto ε é um conjunto de eventos consistindo de uma seqüência $E_0(x)$, $E_1(x)$, . . . , $E_n(x)$ representando planos e ações.

$$\varepsilon = \{ E_0(x), E_1(x), \ldots, E_n(x) \}$$

DEFINIÇÃO 2 (ABSTRAÇÃO)

Sejam dois eventos $Ei(x)$, $Ej(x) \in \varepsilon$. Diz-se que Ej abstrai diretamente Ei se, e somente se, para todo evento Ei, temos Ej, mas o contrário não é válido. O fechamento transitivo é válido e o fato que Ej abstrai Ei é escrito da forma abs(Ej(x), Ei(x)). Portanto, Ej abstrai Ei, se, e somente se, os axiomas de lógica de segunda-ordem abaixo são válidos:

(I) $\forall E_i, E_j \, [abs(E_j(x), E_i(x)) \leftrightarrow (\forall x.E_i(x) \rightarrow E_j(x))]$

(II) $\forall E_i, E_j, E_k \, [abs(E_i(x), E_j(x)) \wedge abs(E_j(x), E_k(x)) \rightarrow abs(E_i(x), E_k(x))]$

DEFINIÇÃO 3 (PASSO FUNCIONAL)

Um passo funcional $f_i(x)$ é uma função unária que faz o mapeamento de um evento em seu respectivo componente

$Ei(x) \rightarrow Ej(x)$, onde $E_i(x), E_j(x) \in \varepsilon$,
Generalizando, temos que: $[f_1(x), f_2(x), \ldots, f_n(x)] : E_i(x) \rightarrow E_j(x)$

DEFINIÇÃO 4 (AXIOMA DE DECOMPOSIÇÃO)

Define-se um axioma de decomposição A_d como:

$$\forall x.E_0(x) \rightarrow E_1(f_1(x)) \wedge E_2(f_2(x)) \wedge \ldots \wedge E_n(f_n(x)) \wedge R,$$

onde $E_0(x), \ldots, E_n(x) \in \varepsilon$, onde $f_1(x), \ldots, f_n(x)$ são passos funcionais, e R descreve as restrições sobre o evento $E_0(x)$.

DEFINIÇÃO 5 (RESTRIÇÃO)

Todo axioma de decomposição tem associado características que agem como restrições sobre toda a estrutura dos eventos. Uma restrição R é um predicado com os valores das restrições V_R sobre qualquer evento E_i. Portanto, todas as restrições devem ser mutuamente consistentes. Cada predicado R é fornecido a partir do axioma

$\forall x.E_i(x) \rightarrow \bigwedge_{j=1}^{n} R_j(V_{R1}(x), V_{R2}(x), \ldots, V_{Rn}(x))$, onde $Ei \in A_d$, e V_R é o predicado de avaliação que representa as restrições.

DEFINIÇÃO 6 (EVENTO FIM)

Um evento é chamado de evento do tipo Fim, escrito da forma fim(x), quando o seguinte axioma é válido:

$fim(x) \leftrightarrow \neg\exists x.\ E_k(x)(abs(E_k(x), E_i(x)))$

O evento Fim é o ponto fixo desta teoria e a implementação segue o seguinte padrão de raciocínio: para cada observação do robô ROFO aplicam-se os axiomas, hipóteses e heurísticas até que uma instância de Fim é alcançada.

DEFINIÇÃO 7 (OBSERVAÇÃO)

Uma observação *O* feita pelo ROFO é uma tupla < E, *R* > , onde E é um evento observado e *R* contém as restrições sobre E; mais formalmente, temos

$O \equiv \exists x.\ E_i(x) \bigwedge_n R_j(V_{R1}(x), V_{R2}(x), \ldots, V_{Rm}(x))$, ainda temos que $S_0 = \{O_1^{-1}, O_2, \ldots, O_n\}$ como sendo o conjunto de observações do ROFO.

DEFINIÇÃO 8 (EXPLICAÇÃO)

Seja Γ um banco de dados e S_0 o conjunto de observações do ROFO, uma explicação de S_0 consiste de todos os modelos μ tal que

(i) $\mu[\Gamma] \not\models \perp$, onde ⊥ é o símbolo de absurdo
(ii) $\mu[\Gamma] \models S_0$

DEFINIÇÃO 9 (PROBLEMA DE RECONHECIMENTO DE PLANOS)

Propriedade de cobertura : Um modelo μ é um modelo coberto quando S_0 gera (vide S_o na definição 7) um evento Fim. Portanto, um modelo μ é um modelo coberto se, $\mu[\Gamma] \models S_0 \wedge fim(x) \in \mu$

Logo, *o Problema de Reconhecimento de Planos* consiste em encontrar os modelos cobertos μ de S_0.

V. MÓDULO REATIVO

Um sistema reativo é de fundamental importância para um robô inteligente móvel com as características que os robôs forenses necessitam, pois um robô móvel precisa reagir rapidamente a qualquer mudança no ambiente. Para isto, o sistema reativo deve ser capaz de comportamentos surpreendentemente complexos, especialmente em tarefas do mundo real como a navegação. Assim, a arquitetura proposta provê o uso de reatividade em seu Sistema Módulo Reativo (SMR), vide figura 2.

A principal vantagem que o SMR integrado ao planejador PIT (veja figuras 2 e 3) tem sobre os planejadores e sistemas reativos tradicionais é que o SMR trabalha robustamente em domínios onde uma modelagem completa e precisa é difícil. Na arquitetura de controle são previstos três níveis de comportamento reativo. O primeiro, o nível da medula espinal, que garante que os arcos reflexos sejam extremamente rápidos. O segundo nível, cerebelo e o bulbo, fornece o controle reativo sensor e motor. A operacionalização das tarefas sensoras e motoras terão bastante influência no tempo de planejamento no nível seguinte. Já o terceiro, nível do córtex cerebral, executa o planejamento orientado à objetivos, o reconhecimento de planos e sistema reativo do robô móvel.

Estruturando os módulos reativos no ROFO:

De forma resumida, torna-se importante estruturar o sistema módulo reativo (SMR) e relacioná-lo com a teoria das ações:

DEFINIÇÕES (REGRAS DE CONTROLE REATIVAS)

Sejam $c_1, c_2, \ldots, c_k$ literais condicionais e $a_1, a_2, \ldots, a_m$ ações.

(R1) Uma regra de controle *simples* possui a seguinte forma:
Se $c_1, c_2, \ldots, c_k$ Então $a_1, a_2, \ldots, a_m$
(R2) Uma regra de controle de *suspensão* é da seguinte forma:
Se $c_1, c_2, \ldots, c_k$ Então SUSPENDE

(R3) Uma regra de controle de *finalização* possui a seguinte forma:
Se $c_1, c_2, \ldots, c_k$ Então PARE

Portanto, uma *regra de controle* só pode apresentar-se nas formas definidas em (R1), (R2) ou (R3). Assim, o SMR é definido como uma coleção de regras de controle.

VI. ESTRATÉGIA DE NAVEGAÇÃO

Navegar significa mover-se pelo mundo: chegar ao destino desejado sem efetuar colisões no meio do caminho, ou seja, planejar rotas. Isto faz com que os problemas de navegabilidade e busca sejam surpreendentemente complexos. O *problema de planejamento de caminho* consiste em traçar um conjunto contínuo de pontos conectando a posição inicial do robô a uma posição desejada.

Se o robô móvel é tão pequeno a ponto de ser considerado um ponto, o problema do planejamento de caminho pode ser solucionado diretamente através da construção de um *grafo de visibilidade*. Este grafo é construído a partir de um conjunto *C* que consiste nas posições inicial e final e também nos vértices de todos os obstáculos. Para formar o grafo de visibilidade, conecta-se todos os pares de pontos em *C* que podem ser vistos uns dos outros, conforme mostra a fig. 4. Depois percorre-se o grafo (usando por exemplo o algoritmo RTA* [7], [10]) para encontrar o caminho ótimo para o robô.

Fig. 4. Construindo um grafo de visibilidade

Todavia, a maioria do robôs, inclusive o ROFO, é de volume não desprezível, e isto precisa ser levado em consideração. Neste caso, considere o ROFO possuindo a forma apresentada conforme figura 5. Este problema pode ser reduzir ao problema anterior de planejamento de caminho.

Fig. 5. Uma nova forma de planejamento de caminho

A idéia básica do algoritmo é reduzir o ROFO a um ponto e executar o planejamento de caminho em um espaço artificial, conhecido como *espaço de configuração*. Para permitir rotações, o robô pode ser representado como uma combinação do ponto P e de um ângulo de rotação Θ. O robô agora pode ser considerado como um ponto que se move através do espaço tridimensional (x, y, z). Os obstáculos também podem ser transformados em objetos tridimensionais do espaço de configuração. Em seguida um grafo de visibilidade pode ser novamente criado e percorrido.

Os passos para redução ao problema de caminhos é o seguinte:

I. Escolha um ponto P na superfície do robô
II. Aumente o tamanho dos obstáculos de forma que eles cubram todos os pontos onde P não pode entrar, por causa do tamanho físico e da forma do robô
III. Construa e percorra um grafo de visibilidade baseado em P e nos vértices do novo obstáculo, conforme mostra a fig. 6.

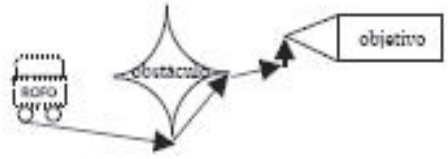


Fig.6. Navegando entre os obstáculos no espaço de configuração

Outro fator importante para navegação do ROFO é utilizar um algoritmo de busca eficiente para encontrar uma boa trajetória, no caso o RTA *.

VII. Conclusão

Este trabalho teve como objetivo central apresentar a integração das tecnologias da Ciência da Computação em aplicações forenses, mais especificamente na atuação diária do perito criminal em local de crime. Com esta finalidade é proposta uma arquitetura de controle para um robô inteligente móvel - RObô FOrense (ROFO). O ROFO é um modelo conceitual baseado no sistema nervoso central do ser humano que utiliza diversas técnicas de inteligência artificial como a estratégia de meios-fins, a regressão de metas, o algoritmo de busca heurística RTA*, a rede neural, o planejamento, a representação do conhecimento e a reatividade, demonstrando aplicações reais da arquitetura de controle de robôs móveis de forma eficiente e funcional no auxílio ao perito criminal.

Referências

[1] Baltes, J.; Liu, X. W. T.; *A An Intuitive and Flexible Architecture for Intelligent Mobile Robots*; 2nd International Conference on Autonomous Robots and Agents; 2004.
[2] Braunl, T.; *Embedded Robotics: Mobile Robot Design and Applications with Embedded Systems*; Springer; 2006.
[3] Choset, H., Lynch, K. M.; *A Principles of Robot Motion: Theory, Algorithms, and Implementations (Intelligent Robotics and Autonomous Agents)*; The MIT Press; 2005.
[4] Leonard, R. J.; *Essential Medical Physiology*, Academic Press; 2003.
[5] Hirose, A.; *Complex-Valued Neural Networks (Studies in Computational Intelligence)*; Springer; 2006.
[6] Luger, F. G; *Artificial Intelligence: Structures and Strategies for Complex Problem Solving*; (5th Edition); Addison Wesley, 2004.
[7] Nogueira ,J. H. M; *Desenvolvimento de Sistemas Computacionais*; Editora Livro Técnico; 2004.
[8] Nogueira, J. H. M; *Inteligência Artificial e a Atividade Pericial*; Revista Perícia Federal, Ano II, p. 30-35; 2000.
[9] Nogueira, J. H. M; *Manipulator Robots Using Partial-Order Planning*; Advances in Artificial Intelligence; p 229-239; Lecture Notes in Computer Science; Springer Verlag; 1998.
[10] Winston, P.; Artificial Intelligence; Addison Wesley; 2005.

José Helano Matos Nogueira tornou-se membro da Sociedade Brasileira de Computação em 1992 e consultor sênior em 1994. Nascido em Fortaleza-Ceará-Brazil obteve seu grau de mestre em Informática pela Pontifícia Universidade Católica do Rio de Janeiro-PUC/Rio, no período de 1993 a 1994. Obteve sua diplomação de Bacharel em Ciência da Computação pela Universidade Estadual do Ceará-UECE, de 1988 a 1992. Em seguida, de 1999 a 2000, obteve a Licenciatura Plena em Matemática pela mesma Universidade Estadual do Ceará-UECE.

Professor, cientista, perito em crimes por computador e computação científica na área de alta tecnologia do governo federal. Foi pesquisador de desenvolvimento científico regional do CNPq, tendo iniciado sua carreira de pesquisador no meio científico nacional desde o ano de 1995. Lecionou em diversas universidades e instituições de nível superior brasileiras, dentre elas ANP/DPF, UFC/CE, UECE/CE, FURG/RS, PUC/RJ. Orientou uma gama de alunos nas mais diversas áreas da Ciência da Computação e Informática, tais como: Informática Forense, Combate aos Crimes por

Computador, Inteligência Artificial, Engenharia de Software, Análise e Projeto de Sistemas, Linguagens de Programação, Banco de Dados. Já publicou dezenas de trabalhos científicos em livros, revistas, congressos, conferências e simpósios, tendo sido premiado em âmbito nacional e internacional, com vários de seus trabalhos. Como profissional aplicado ao desenvolvimento de sistemas, sua equipe criou sistemas computacionais para empresas de pequeno, médio e grande porte, iniciando com a metodologia estruturada e depois evoluindo para abordagens da orientação a objetos e dos paradigmas de representação do conhecimento.

Atualmente, trabalha na Polícia Federal brasileira dedicando-se no combate aos crimes por computador, crimes cibernéticos e crimes de alta tecnologia que de alguma forma têm assolado a sociedade.

Estudo de taxonomia de ataques e atacantes em um honeypot de alta interação

Laerte Peotta de Melo Dino Macedo Amaral,

***Resumo*—Este estudo tem o propósito de divulgar informações de ataques e taxonomia destes, mensurando os tipos de ataques e determinando de forma clara e concisa o que leva um atacante a criar técnicas e procurar sistemas vulneráveis.**

***Palavras-chave* Hackers, honeypots, segurança da informação, spams, proxy**

***Abstract*—This study it has the intention to divulge information of attacks and taxonomy of these, quantify the types of attacks and determining of clear and concise form what it takes an aggressor to create techniques and to look vulnerable systems**

***Keywords*— Hackers, Honeypots, information security, spam, proxy**

I. Introdução

A necessidade de integração dos variados dispositivos de segurança da informação torna-se imperativo para um ajuste fino dos mesmos. Firewalls, IDS, Honeypots, Honeynets, Antivírus, Anti-Spam devem funcionar como "amigos" em que os dados coletados por um dispositivo são compartilhados com os outros, no intuito de gerar informações que ajudem a realimentar as suas respectivas bases de assinaturas. Neste sentido, precisamos que os dispositivos estejam configurados a gerar *logs*, uma condição *sine qua non* para obter informações que, com auxílio de ferramentas apropriadas, iremos nos pautar para minimizar os impactos causados por possíveis ataques a nosso ambiente interno. Dentre os dispositivos mencionados, destacaremos os *honeypots* que possuem a específica atividade de gerar *logs* dos eventos ocorridos em seu ambiente.

O objeto deste artigo é expor os métodos mais utilizados para tentativa de comprometimento de máquinas conectadas a internet. Analisaremos informações coletadas entre os dias 28 de janeiro a 14 de setembro de 2005, as quais foram obtidas diretamente de uma máquina montada utilizando metodologia de *honeypots*, evitando, caso haja o comprometimento, de que a mesma fosse usada como ponto inicial de algum outro ataque a servidores e usuários da internet. Analisaremos, também, alguns pontos de taxonomias desses ataques, bem como a finalidade destes. Não iremos descrever a topologia de rede utilizada, nem os equipamentos e softwares, pois o fato relevante, aqui exposto, é principalmente levantar quais serviços são mais vulneráveis e mais cobiçados pelos atacantes e montar um perfil dos motivos dos eventos ocorridos .

Laerte Peotta – Universidade Católica de Brasilia (peotta@peotta.pr.br)
Departamento de pós-graduação – Laboratório de segurança de redes.
Dino Amaral– Universidade de Brasília , Departamento de Engenharia Elétrica – Faculdade de Tecnologia.

II. Honeypots de Alta Interação

Os *honeypots* de alta interação fornecem um sistema operacional completo e aplicativos na qual os atacantes poderá intergir com os mesmos. Este tipo de *honeypot* não nenhum serviço, ao invés disto, eles são computadores reais com aplicações para ser burladas, invadidas e consequentemente gerar informações. Além de permitir detectar eventos de solicitações ao sistema, com os honeypots de alta interação é possível ao atacante burlar os serviços disponíveis no host e obter acesso ao sistema operacional. Com esta interatividade, podemos capturar os *uploads* dos rootkits que o atacante que instala no sistema, analisar o que é digitado por ele quando o mesmo possui acesso ao host comprometido e monitorar suas comunicações com outros atacantes em salas de chat, usados pelos mesmos para compartilhar os seus intentos pela rede mundial de compuatdores. A partir desta coleta, podemos ter idéia dos aspectos motivacionais dos atacantes, seus níveis de conhecimentos, metodologia e outras informações críticas.

Os honeypots de alta interação são projetados para capturar tráfegos desconhecidos, inesperados, toda esta capacidade não é adquirida facilmente, existe um preço a ser pago.

a) São expostos a um alto nível de risco, visto que os mesmos podem usados para disparar ataques a outros sistemas, quando comprometidos;
b) São complexos, pois a simples instalação de softwares não condiciona a existência de um honeypot. É necessário que um sistema real seja instalado e configurado para os atacantes possam intergir com os sistemas. O grau de complexidade aumenta na medida que é necessário que se minimize os riscos dos honeypots, embora os mesmos forneçam serviços vulneráveis.

A seguir, uma breve comparação de honeypots de alta interação e baixa interação, as diferenças servem de parâmetros para uma escolha de qual tipo de *honeypot* melhor se encaixa em suas aspirações para as pesquisas a serem realizadas.

Tabela 1 – Comparação entre tipos de honeypots

Honeypots de baixa interação	Honeypots de alta interação
Fácil de instalar e configurar	Pode ser complexo de instalar e configurar (versão comerciais são mais simples)
Riscos controlados com serviços emulados controlando o que o atacante pode fazer ou não	Riscos são aumentados, pois os atacantes são confrontados com um sistema operacional real para interagir.
Captura limitada de informações devido a limitação de interatividade	Pode capturar mais informações, incluindo novas ferramentas, dados de comunicação e o que foi digitado durante a interação com o honeypot.

III. Taxonomia dos ataques

A. Coleta dos eventos

Em uma taxonomia de honeypots, a coleta de dados consiste em extrair informações dos arquivos de *logs*. É fundamental para a perícia computacional, pois, através de várias linhas de *logs* podemos de ter idéia em quais circunstâncias os ataques ocorreram. Todas as informações foram coletadas e catalogadas em relação aos tipos de ataques utilizando o software Snort[1] em sua versão 2.1 . Em um primeiro instante, mapeamos os endereços IP´s, tanto de origem como de destino, dos eventos capturados em nosso honeypot.

Tabela 2 – Endereços IP - total dos *logs* analisados

Total de eventos	**860**
IP de Origem	**192**
IP de destino	**8**

B. Distribuições de eventos por protocolo

O tráfego de rede capturado pelo *honeypot* segue o formato de pacote do protocolo TCP/IP. Quando a comunicação entre 2(duas) estações é estabelecida, a mesma acontece sob as regras de um protocolo (um conjunto de regras) compreendido por ambas as partes e a suíte TCP/IP define o protocolo usados na Internet. Neste tópico, faremos uma breve explanação sobre tópicos, tidos como relevantes, para uma análise posterior dos eventos correlatos ao protocolo TCP/IP.

Os protocolos disponíveis na pilha TCP/IP mostram como o tráfego está se comportando na rede. Para efeitos deste artigo, analisaremos o comportamento de 3 protocolos, a saber : TCP, UDP e ICMP.

O protocolo TCP é orientado a conexão, fornecendo uma confiabilidade maior na conexão entre dois *hosts*. A exploração de vulnerabilidade deste protocolo consiste em manipular os dados do cabeçalho TCP (Figura 1) de forma a tirar proveito de alguma vulnerabilidade existente. Para exemplificar, podemos usar as *flags* do TCP para enviar um tráfego malicioso, com todas as *flags* setadas, o que não faz sentido visto que terámos os *flags* FIN, RST e SYN setados, já que a flag SYN denota o início de uma conexão e os flags RST e FIN denotam o término de uma conexão.

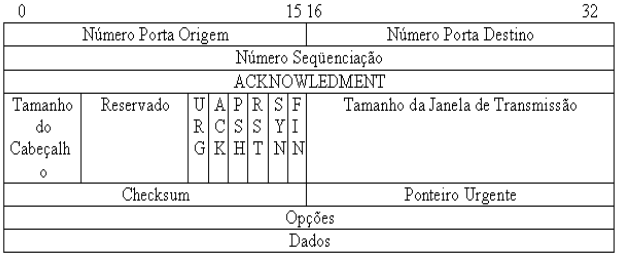


Figura 1 – Cabeçalho TCP

UDP é um protocolo não orientado a conexão, na qual fornece um serviço não-confiável, sem controle de fluxo, sem recuperação de erro para os serviços que se utilizam deste protocolo. Por causa desta simplicidade, o cabeçalho UDP possui um tamanho menor e consome menos recursos da rede em comparação como TCP. O protocolo UDP é utilizado em situações em que os mecanismos de confiança, como os do TCP, não são necessários.

Podemos citar casos onde os controles de fluxo e de erro são realizados pelas camadas acima da camada de transporte e em situações de comunicações em tempo real, como as de jogos *online* e videoconferência. A seguir, alguns protocolos que usam o protocolo UDP para transporte :

1) TFTP : É semelhante ao FTP porém sem confirmação de recebimento pelo destino ou reenvio.
2) SNMP : É utilizado para gerenciar dispositivos de rede, como *switches* e roteadores. Os dados são obtidos através de requisições de gerente a um ou mais agentes. O problema é que os *hackers*, utilizam este protocolo para obter informações sobre o sistema, como as tabelas de roteamento. As últimas versões do SNMP podem usar criptografia md5, porém a maioria ainda usa versões antigas que pemite a senha em formato de texto.
3) DHCP : É utilizado em redes que sofrem constantes alterações na topologia e o administrador não pode verificar o IP (*Internet Protocol*) de cada máquina devido a enorme quantidade, então o roteador distribui IPs automaticamente para as estações. Como esta atribuição é feita com a utilização do UDP, caso haja algum problema o usuário terá que pedir o reenvio ou reiniciar a máquina.
4) DNS : Um tradutor dos nomes na rede, na qual cada IP pode ser correspondido com um nome. Neste caso, imaginemos que um usuário esteja acessando a internet e deseja ir para outra página. Ele digita o endereço no campo apropriado e entra. Se a página, por acaso, não abrir por não ter reconhecido o endereço, o problema poderá ter

[1] www.snort.org

sido no envio ou resposta do servidor de nomes utilizando o UDP, e então o usuário tentará de novo acessar a página e provavelmente conseguirá.

O protocolo ICMP é usado de maneira unidirecional para enviar mensagens para o *host*. Não nenhum tipo de autenticação, o que permite que o protoloco ICMP seja alvo de ataques de negação de serviço. Enumeramos aqui alguns ataques que utilizam o protocolo ICMP :

1. Ataque DoS ICMP : O atacante usa as mensagens "*Time Exceeded*" ou "*Destination Unreachable*" , que faz com que o *host* termine imediatamente uma conexão. Ao interceptar uma conexão entre 2 (dois), o atacante usa deste artifício enviando mensagens para um dos hosts, o que causa um término da comunicação entre ambos.
2. ICMP Smurf: O atacante envia um pacote forjado ICMP de requisição para endereços de broadcast , como resposta todos os endereços da rede envia uma pacote ICMP de resposta para a vítima
3. Ping da Morte: Envia de uma pacote ICMP com um tamanho maior que o normal. Como o sistema operacional não consegue efetuar a remontagem do pacote, o sistema sofre um "reboot" ou mesmo um travamento.
4. Inundação de Ping: Uma quantidade grande de requisições ICMP (*ICMP Echo request*) , que sobrecarrega o sistema alvo, limitando os seus recursos computacionais para responder às requisições, dificultando assim o acesso a rede.

Na captura realizada , temos as seguintes estatísticas no tocante ao tipo de protocolo usado nos diversos eventos capturados pelo Snort.

Tabela 2: Eventos por protocolo

Porcentagem	Número eventos	Protocolos
71.98 %	619	TCP
27.67 %	238	ICMP
0.35 %	3	UDP

IV. Distribuição de eventos por criticidade

Os ataques, aqui descritos, serão divididos em três tipos básicos: Baixo, Médio e Alto, onde podemos definir como:

A. Baixo

Um ataque definido com severidade baixa é todo aquele que chega ao servidor e que não prejudica de qualquer maneira os serviços que estejam rodando na máquina. Um exemplo seria a utilização da ferramenta Cyberkit[2] que apenas coleta informações de diversos aplicativos como ping, tracetoute, finger, whois entre outros.

B. Médio

Ataques catalogados como severidade média são ataques que não possuem a qualidade necessária para comprometer um sistema. No exemplo, podemos citar um ataque de scanner utilizando a ferramenta NMAP[3], que busca por serviços disponíveis na estação remota. Essa técnica constitui, geralmente, um passo inicial na anatomia de um ataque real, pois busca também por serviços que possam estar vulneráveis na estação remota.

C. Alto

Ataques de severidade alta são ataques que permite a um hacker obter acesso total à máquina, podendo instalar ferramentas, fazer *downloads*, criar contas para novos usuários e restringir acesso a outros usuários legítimos do sistema.
Um exemplo desse tipo de ataque seria um envio de *shellcode* tentando obter acesso a uma área de memória que permitisse o atacante a executar comandos de forma remota

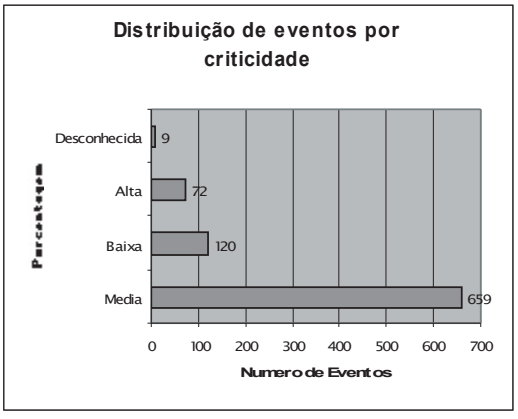


Gráfico 1: Relação de criticidade dos ataques

V. Distribuições de ataques por hora

Em uma análise dos eventos ocorridos, podemos levantar a informação de qual horário, durante um período de 24 horas, o host ou serviço está sujeita a um maior número de ataques. A intenção desta abordagem não é precisar o horário dos eventos, mas fornecer subsídios suficientes para a montagem de um quadro de análise em que podemos nos pautar para implementar uma política de segurança mais eficaz. Como exemplo, podemos citar um caso de escolha de horário para atualizações do sistema operacional e outros sistemas correlatos que estão instalados em nossos dispositivos de segurança. Convém afirmar que a criticidade da atualização pode ser o fator determinante para a realização da mesma, porém não devemos deixar de lado as estatísticas no tocante ao horário e evitar períodos de maior incidência de ataques, onde teoricamente estaríamos mais vulneráveis a eventos que

[2] www.cyberkit.net

[3] www.insecure.org/nmap/

possam causar algum dano a nosso ambiente interno.
Na coleta de dados realizada, não houve uma disparidade da incidência de ataques no período analisado, observamos menor incidência de ataques foram no horário de 1h com 1,63% do total de eventos e a maior incidência, no horário de 12h com 8,26 %.

É conhecido que vários fatores podem distorcer esta informação, mas podemos ter uma boa aproximação, pois as variáveis foram coletadas durante o período de quase um ano.

Como são mostradas no gráfico 2, as informações estão espalhadas durante todo o dia, não tendo uma base ou definição clara em qual horário seria um foco maior de ataques.

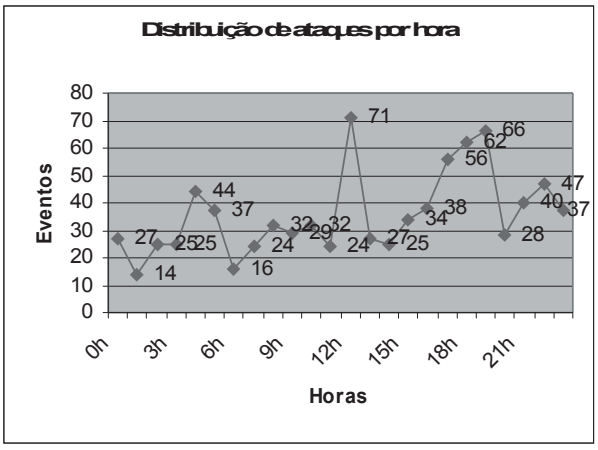


Gráfico 2: Ataques por hora

VI. Distribuições de eventos por portas

Cada processo que deseja estabelecer uma comunicação com outro processo identifica na suíte de protocolo TCP/IP uma ou mais portas. O conceito de portas, na suite de protocolo TCP/IP, refere-se à um mapeamento interno que a estação realiza para possibilitar a comunicação entre hosts em vários processos simultaneamante com finaliades diversas, como por exemplo um transferência de arquivos via FTP (File Transfer Protocol) na porta 21 e um acesso remoto via Telnet na porta 23. A porta é um número de 16 bits, existem 2 tipos de portas :

1. Portas conhecidas : As portas conhecidas pertencem aos serviços padrões, e seus números variam de 1 a 1023. A maioria dos serviços requer somente uma porta, porém temos algumas exceções como BOOTP (*Bootstrap Protocol*), que usa as portas 67 e 68, e os serviços de FTP, que usa as portas 20 e 21. Estas portas são controladas e assinaladas pela IANA (*Internet Assigned Number Authority*). A razão para deste tipo de porta é permitir que os clientes possam se conectar aos servidores sem a necessidade de configuração.
2. Efêmeras: os clientes não precisam saber os números das portas conhecidas, pois os mesmos iniciam a comunicação com os servidores e o número da porta que eles estão usando é contida nos datagramas UDP que são enviados ao servidor. Os valores destas portas variam de 1024 a 65535, o cliente pode usar qualquer número, mas obedecendo a combinação de protocolo de transporte, endereço IP (*Internet Protocol*) e número da porta seja único. As portas efêmeras não são controladas pela IANA e podem ser usadas pelos desenvolvedores as portas que melhor convier para suas aplicações.

O ataque por portas nos dá uma boa visão do que está sendo procurado pelos atacantes, pois a correlação existente entre o número da porta e o serviço disponibilizado pela mesma nos leva a conclusões sobre os alvos procurados pelos atacantes. A busca por vulnerabilidades é um dos passos iniciais na anatomia de um ataque, e o mesmo acontece com o uso de *scanner,* que com a emisão de pacotes e a suas respectivas respostas compõem um quadro de vulnerabilidade no alvo em questão.

No gráfico 3 podemos ver claramente que a porta 1080 é uma das mais sondados, isso se dá em razão de atacantes à procura de *proxies* vulneráveis para envio de mensagens não solicitadas, comumente chamado de SPAM.

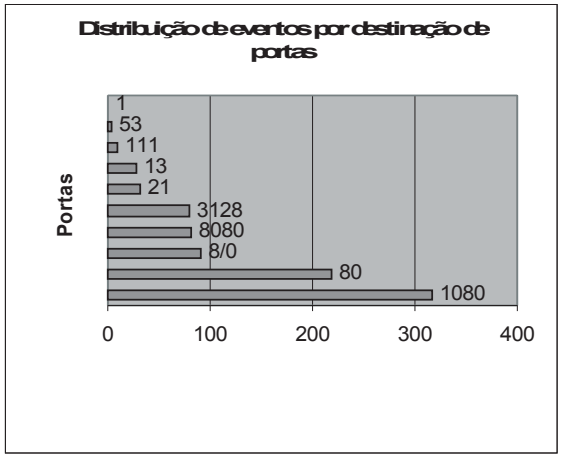


Gráfico 3: Eventos por portas

Abaixo segue uma tabela com as portas e respectivos ataques capturados. Somando os eventos ocorridos nas portas 1080 e 8080, temos 43,49% dos ataques de *Scan Proxy* . Na porta 80, que teve 25,47% do total de ataques, embora a diversidade dos ataques nos causasse dificuldade adicional para uma análise mais criteriosa, podemos constatar que o alvo era o servidor de Web IIS (Internet Information Service). Quanto a descrição dos ataques, mais adiante nos atentaremos aos ataques com maior incidência em nosso ambiente.

Tabela 3: Eventos por portas

Porcentagem	Eventos	Porta	Ataques
35.23	303	1080	Scan Proxy
8.26	71	8080	Scan Proxy
8.26	71	8/0	ICMP Nmap
5.23	45	3128	Scan Squid
5.00	43	80	WEB-IIS

VII. Métodos de ataques: os 5(cinco) ataques com maior incidência.

Os métodos de ataques podem variar devido a várias circunstâncias, como vulnerabilidades críticas, *exploits* para serviços conhecidos ou mesmo um ataque direcionado.

Na tabela seguinte podemos ver que 43,49% dos eventos foram do tipo de Scan Proxy Attempt. Neste tipo de ataque, o objetivo não é o comprometimento do sistema, e sim o uso de servidores *proxies* para acessar outros *sites* na Internet. Esta situação advém da técnica usada pelo atacantes de ocultar os seus endereços IP (*Internet Protocol*) para dificultarem o rastreamento do mesmo, visto que nos arquivos de *log* é registrado o endereço IP (*Internet Protocol*) do servidor *proxy* que realiza intermediação do *host* com a internet. Quanto aos outros tipos de ataques, de menor incidência, os mesmos consistem em um dos passos iniciais na anatomia dos ataques até então conhecidos, que procuram por sistemas vulneráveis que sirvam de ponto inicial para deslanchar as suas atividades na grande rede.

Tabela 4: Maiores incidência de ataques

Porcent.	Eventos	Tipo de ataque	Criticidade
43.49	374	SCAN Proxy attempt	Média
16.51	142	ICMP PING NMAP	Média
6.51	56	ICMP Destination Unreachable	Baixa
5.23	45	INFO - Possible Squid Scan	Média
5.00	43	WEB-IIS view source via translate header	Média

VIII. Origens que mais atacaram

Em uma separação por *hosts*, foram coletados os cinco hosts que mais atacaram nosso sistema.

Tabela 5: Eventos por origem de ataques

host	eventos	%	País
83.102.136.102	65	7,56	Russia
65.75.178.200	62	7,21	California
211.158.6.87	51	5,93	China
200.252.123.5	40	4,65	Brasil
200.252.84.51	40	4,65	Brasil

O campo porcentagem referencia-se apenas parte do total de eventos, haja vista que muitos estão abaixo do mínimo. Nas informações coletadas tivemos ataques partindo de 192 hosts distintos.

IX. Conclusão

Neste artigo foi analisado eventos coletados em uma máquina colocada diretamente na internet e funcionando como um *honeypot*. Constatatou-se que a taxonomia dos ataques pode ter suas ações pontuadas e definidas de acordo com critérios práticos, claros e previamente definidos. As ações de atacantes, neste caso, foram em sua maioria, envio de mensagens não solicitadas. Grande parte das informações que chegaram até o servidor partia de ferramentas e processos automatizados, haja vista a velocidade das ações e o fato do servidor não ter nenhum registro de domínio válido, ou seja, simplesmente estava com um ip válido para a internet e aguardando.

Considerou que todo o tráfego que chegou até o sistema seria catalogado como sendo malicioso, pois nenhum serviço que estava atendendo era específico para este fim.

Pretende-se publicar, em breve, outro artigo descrevendo de forma sucinta, a topologia e todas as ferramentas e sistemas utilizados.

A intenção deste artigo não é a de esgotar o assunto e sim de informar e divulgar.

X. Referências Bibliográficas

[1] Spitzner , Lance 2002, Honeypots: Tracking Hackers, Publisher: Addison-Wesley Professional (September 10, 2002) Language: English ISBN: 0321108957

[2] Peotta, Laerte e Mendonça, Érico (2004). Honeynets. Monografia Universidade Católica de Brasília, Segurança em redes de computadores

[3] HONEYNET.BR: DESENVOLVIMENTO E IMPLANTAÇÃO DE UM SISTEMA PARA AVALIAÇÃO DE ATIVIDADES HOSTIS NA INTERNET BRASILEIRA Honeynet.BR Team Instituto Nacional de Pesquisas Espaciais – INPE

Questões legais do uso da certificação digital na proteção dos direitos de autor de programa de computador

Hélio Santiago Ramos Júnior

***Abstract*—**Este trabalho se propõe a discutir eventuais implicações legais relativas ao uso da certificação digital na proteção dos direitos de autor de programa de computador em virtude da possibilidade de adoção de um modelo de proteção de programa de computador por certificação digital proposto na Universidade Federal de Santa Catarina com o objetivo de coibir de forma mais eficaz a pirataria de programa de computador.

Palavras-chave—Programa de computador, certificação digital, direito do consumidor.

I. INTRODUÇÃO

No Brasil, a Lei 9.609, de 19 de fevereiro de 1998, conhecida como lei do software, dispõe sobre a propriedade intelectual do programa de computador bem como sua comercialização no país. Ela traz, em seu artigo primeiro, o conceito jurídico de programa de computador e, no seu art. 12, tipifica como crime específico a violação de direito de autor de programa de computador.

A doutrina faz distinção entre programa de computador e software, considerando que este último difere do programa de computador na medida em que o seu conceito é mais abrangente, podendo ser utilizado para se referir, além do programa de computador, também aos seus acessórios que inclui os materiais de apoio relacionados ao programa.

Neste sentido, "software abrange, além do programa de computador em si, que é a linguagem codificada, também a descrição detalhada do programa, as instruções codificadas para criar o programa, a documentação escrita auxiliar deste, bem como outros materiais de apoio relacionados"

(Wachowicz, 2004, p. 71)

Esta diferença é importante porque o programa de computador é protegido pela Lei 9.609/98 enquanto que os materiais de apoio relacionados ao programa, sendo considerado obras intelectuais, são tutelados pela Lei 9.610/98 (Lei de Direitos Autorais).

Em 2001, um modelo de proteção de programa de computador por certificação digital foi proposto por João Luiz

Francalacci Rocha em uma banca de mestrado no Centro de

Ciências da Computação da Universidade Federal de Santa Catarina com a finalidade de propor uma forma mais eficaz de combate à pirataria de programa de computador.

De modo geral, este modelo de proteção tem como principal característica o fato de vincular o registro da licença de uso do programa de computador ao certificado digital do usuário para impedir o uso não autorizado e a comercialização ilegal de cópia de programa de computador.

Naquela ocasião, o próprio autor reconheceu que ainda há muito que ser feito para viabilizar a proteção de programa de computador por certificação digital, neste sentido, salientou que "a questão jurídica que envolve o termo de contrato entre produtor e usuário também deve ser alvo de pesquisa no campo do direito, respeitando, claro, o lado do consumidor, mas provendo termos legais e eficazes que reforcem a aliança entre o usuário, software e certificados". (Rocha, 2001, p. 75).

De tal sorte, dada a importância do tema, o presente trabalho se propõe a examinar a compatibilidade do modelo de proteção de programa de computador proposto por Rocha com as normas do ordenamento jurídico brasileiro, principalmente no que concerne aos direitos do consumidor, refletindo sobre suas implicações legais e, ao final, propõe-se alternativas para solucionar os problemas identificados, visando a sua adequação à lei.

II. A CERTIFICAÇÃO DIGITAL E A ICP-BRASIL

Antes de comentar sobre o modelo de proteção de programa de computador por certificação digital, é fundamental aprofundar um pouco o estudo sobre a criptografia, o contrato eletrônico e a assinatura digital para um melhor esclarecimento sobre a certificação digital e como ela poderá contribuir para proteger os direitos de autor de programa de computador.

A. A criptografia

O Instituto Nacional de Tecnologia da Informação (ITI) define a criptografia como sendo "um ramo das ciências exatas que tem como objetivo escrever em cifras. Isso ocorre em função de um conjunto de operações matemáticas que transformam um texto claro em um texto cifrado".

A criptografia é utilizada para evitar a violação de uma informação constante em um documento, através da transmissão de um texto cifrado pelo emissor para o receptor o qual, ao receber o documento cifrado, decifra-o, tornando-o,

assim, legível o conteúdo do texto emitido.

Em 2000, Corrêa já havia observado a importância da criptografia, apontando, inclusive, dentre as diversas vantagens da sua utilização, por exemplo, a possibilidade de contribuir para a proteção da propriedade intelectual: "Por que precisamos da criptografia na grande rede? Por vários motivos; dentre eles poderíamos citar: tornar original uma mensagem enviada por correio eletrônico, mediante a utilização de assinaturas digitais; tornar documentos pessoais inacessíveis e, assim, privados; verificar a identidade de outra pessoa online, que esteja acessando a rede; verificar a fonte provedora de um arquivo que está sendo copiado, em outras palavras, tornar o download mais seguro; proteger transações financeiras; habilitar o fluxo de caixa digital na internet; proteger a propriedade intelectual; evitar opiniões ilegais e puni-las; proteger a identidade e a privacidade de todos" (p.82).

Embora a criptografia seja um método bem antigo de codificar mensagens, a tecnologia veio a utilizar suas técnicas para dar soluções a problemas hodiernos, passando a garantir não somente a privacidade e o sigilo de documentos, mas, também, adaptou-se no sentido de preservar a integridade e autenticidade do documento eletrônico.

Diante dos constantes avanços tecnológicos e do emprego cada vez maior das tecnologias da informação, pode-se dizer que existe uma grande possibilidade de se explorar e elaborar mecanismos que contribuam para impulsionar ainda mais o desenvolvimento da sociedade, no entanto, deve-se atentar para a proteção dos direitos fundamentais do cidadão em face das novas tecnologias.

Há dois tipos de criptografia que são a simétrica e a assimétrica.

A criptografia simétrica funciona com a utilização de duas chaves idênticas, ou seja, a chave para cifrar e a chave para decifrar um documento são a mesma de modo que o emissor assim como o receptor devem conhecer o segredo da chave.

Logo, para garantir a privacidade da informação transmitida, faz-se necessário que apenas ambos conheçam a chave. Portanto, na criptografia simétrica, por se tratar de uma mesma chave, qualquer receptor que tiver conhecimento da chave secreta poderá alterar o documento por ser esta chave correspondente a mesma tanto para sua cifração quanto para decifração.

Ao contrário da criptografia simétrica, a criptografia assimétrica, por sua vez, "utiliza um par de chaves diferentes entre si, que se relacionam matematicamente por meio de um algoritmo, de forma que o texto cifrado por uma chave, apenas seja decifrado pela outra do mesmo par" (ITI).

Na criptografia assimétrica, a chave que o emissor utilize para cifrar seu documento é denominada chave privada e deve ser de seu exclusivo conhecimento, enquanto que a chave pública é aquela que pode ser fornecida ao público, pois o conhecimento da chave pública apenas permite a leitura do documento e não a sua alteração.

Há algumas desvantagens que podem ser apontadas no que concerne ao uso da criptografia, como, por exemplo, a possibilidade de utilizá-la para a troca de mensagens entre criminosos com o objetivo de violar a lei.

Acontece que os agentes que utilizam a criptografia para a troca de mensagens não são obrigados a produzir prova contra si mesmos. Além disso, mesmo se houvesse uma determinação judicial autorizando a quebra do sigilo destas mensagens para o fim de investigação criminal ou instrução processual penal, isto seria uma tarefa muito difícil.

Esta dificuldade está consubstanciada no fato de que os programas de criptografia são potentes e a sua quebra demoraria alguns anos o que possivelmente levaria à prescrição dos supostos delitos que tenham sido cometidos, sendo que os infratores poderiam ainda ser inocentados com base no princípio de que, na dúvida, deve-se inocentar o réu, uma vez que não se teria conhecimento do conteúdo da mensagem privada.

A relevância deste assunto que envolve a segurança nacional em face do uso da criptografia por criminosos e terroristas foi o tema central de ficção científica na obra "Fortaleza Digital", onde o autor explica bem a noção de criptografia:

"A codificação por chave pública era um conceito ao mesmo tempo simples e brilhante. Consistia no uso de um programa simples, para computadores pessoais, que alterava as mensagens de e-mails de tal forma que estas se tornavam impossíveis de ler. Os usuários passaram a poder escrever suas mensagens e codificá-las usando um programa desse tipo. O texto resultante parecia um bloco de caracteres aleatórios e sem sentido: um código. Qualquer um que interceptasse a mensagem iria ver apenas lixo em sua tela. A única maneira de decifrar o código era digitar a senha do remetente - uma série secreta de caracteres que funcionava basicamente como a senha de um cartão de crédito. Geralmente, as senhas eram longas e complexas e transportavam as informações para transmitir ao algoritmo de decodificação as operações matemáticas necessárias para recriar a mensagem original. Os usuários desses programas voltaram a poder, então, enviar emails com total confiança. Mesmo se a transmissão fosse interceptada, apenas aqueles que tivessem a chave poderiam decifrá-la" (Brown, 2005, p. 27).

B. O contrato eletrônico

A ausência de leis nos países referentes ao comércio eletrônico fez surgir a Lei-Modelo da UNCITRAL sobre comércio eletrônico que estabeleceu princípios para auxiliar os países na criação de suas legislações internas sobre o tema.

Dentre estes princípios, destacam-se "o reconhecimento das informações e das mensagens de dados e a igualdade entre o documento eletrônico e os registrados em papel; o reconhecimento legal da assinatura digital; a notificação de recibo de documentos, tempo e lugar de despacho e de recibo das mensagens de dados". (Leite, 2003, p.226).

O desenvolvimento do comércio auxiliado principalmente pela crescente utilização da Internet como um meio de

comunicação trouxe como conseqüência a necessidade de celebração de contratos através do meio eletrônico.

O contrato eletrônico deve ser compreendido como sendo um negócio jurídico celebrado através de meios eletrônicos onde as partes manifestam a vontade de assumir um compromisso recíproco e honrar com as disposições acordadas.

Há muitos contratos eletrônicos que consistem em contratos de adesão, ou seja, contratos preestabelecidos unilateralmente cujas cláusulas não foram discutidas nem acordadas entre as partes. Em geral, estes contratos recebem a denominação de clickwrap tendo em vista que o usuário manifesta a aceitação das cláusulas contratuais com um simples click do mouse.

Os contratos eletrônicos de adesão consistem em negócios jurídicos celebrados através do meio eletrônico onde diversas empresas oferecem seus serviços ou produtos e apresentam um contrato com as cláusulas preestabelecidas.

Deste modo, em se tratando de contrato de adesão, o usuário contratante, caso queira utilizar os produtos ou serviços da empresa, não tem outra alternativa senão se submeter a aceitar as cláusulas que constam no contrato as quais não foram acordadas entre ambos mas sim imposta por uma das partes contratantes, cabendo a outra apenas aceitar o contrato na íntegra ou recusá-lo.

O usuário contratante deve estar atento às cláusulas contidas nos contratos eletrônicos de adesão, e, por estas cláusulas contratuais serem estabelecidas unilateralmente, "deve-se recusar validade àquelas que sejam abusivas, isto é, que causem manifesto desequilíbrio do contrato, por reduzirem unilateralmente as obrigações do predisponente (a parte mais forte), em prejuízo dos clientes, ou por agravarem as destes, de forma que seja socialmente sentida como ilegítima" (Noronha, 2004, p.34).

Em relação à forma de manifestação de vontade nos contratos eletrônicos de adesão, especialmente naquela onde se considera o aceite dos termos através do click do mouse, cabe a observação de que "este tipo de declaração, que em muitos casos implica, inclusive, em renúncia a direitos, não pode ser manifesto apenas por um simples click, como nos contratos clickwrap" (Ventura, 2001, p. 68).

Há questões relativas aos contratos eletrônicos que devem ser esclarecidas pelo direito para a perfeita caracterização e identificação da celebração de um contrato eletrônico. Por exemplo, em se tratando dos contratos eletrônicos celebrados através da troca de e-mails, entende-se que há, neste caso, contratação entre ausentes por ser similar a uma contratação por correspondência.

Assim, quando se trata dos contratos entre ausentes, "o ordenamento jurídico brasileiro adota a teoria da expedição, ou seja, o contrato oriundo da troca de e-mails estaria formado no momento em que o oblato expedisse sua resposta aceitando os termos da proposta (anteriormente encaminhada por email)" (Glitz, 2003, p.190).

Há diversas preocupações ao se realizar uma celebração de um contrato por meio eletrônico, dentre estas, destaca-se a questão de identificação das partes e da integridade do conteúdo dos documentos eletrônicos por não haver a possibilidade de confirmação do endereço físico, veracidade da identidade e capacidade jurídica dos contratantes.

A respeito da integridade do documento, aponta-se a possibilidade da alteração do documento eletrônico, da alegação de não recebimento, ou de recebimento com conteúdo diverso do enviado, e de se interceptar informações contidas remetidas eletronicamente.

Desta forma, "percebe-se a importância de conseguir garantir que estes não sofreram alterações posteriores a sua concepção. Busca-se então a certeza da integridade do documento, para que possa haver também a certeza de que o conteúdo permaneceu inalterado" (Hammes, 2004, p.43).

C. Os documentos eletrônicos e a assinatura digital

A atribuição de valor probatório aos documentos eletrônicos é um dos pressupostos para que se possa garantir uma segurança nas atividades desenvolvidas eletronicamente, pois, sendo o documento eletrônico considerado válido como meio de prova, ele poderá ser utilizado, por exemplo, para provar a existência de um negócio jurídico.

No art.212, inc. II do Novo Código Civil, tem-se que "salvo o negócio a que se impõe forma especial, o fato jurídico pode ser provado mediante: II - documento". Pode-se entender que este termo documento expresso no Código Civil brasileiro tenha um sentido amplo o que permitiria a utilização do documento eletrônico como meio de prova.

Há também o princípio da livre apreciação de provas pelo juiz, neste caso, se o juiz confiar na autenticidade do documento eletrônico, poderá considerá-lo como meio de prova válido.

Assim, conforme consta no art. 131 do Código de Processo Civil: "O juiz apreciará livremente a prova, atendendo aos fatos e circunstâncias constantes dos autos, ainda que não alegados pelas partes; mas deverá indicar, na sentença, os motivos que lhe formaram o convencimento".

Ainda, o Código de Processo Civil de 1973, no caput de seu art. 332, estabelece que "todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa".

Desta forma, o Código de Processo Civil permite a abrangência de outros meios de prova desde que sejam meios legais e moralmente legítimos, assim, ao se garantir a integridade e autenticidade dos documentos eletrônicos, eles passam a ser dignos de eficácia probatória.

A Medida Provisória n. 2.200/01 criou a Infra-Estrutura de Chaves Públicas (ICP-Brasil) e teve como objetivo dar validade aos documentos eletrônicos, e, em seu art.10, caput, considerou-os como documentos públicos ou particulares para todos os fins legais.

Estabeleceu ainda uma presunção de veracidade para os documentos eletrônicos que forem assinados digitalmente e que utilizassem os certificados da ICP-Brasil. Desta forma, os documentos eletrônicos passam a ter a mesma validade

jurídica dos documentos em papel.

De acordo com o ITI, a assinatura digital pode ser conceituada como "uma modalidade de assinatura eletrônica, resultado de uma operação matemática que utiliza algoritmos de criptografia assimétrica e permite aferir, com segurança, a origem e a integridade do documento".

Acerca deste assunto, comenta Blum (2002, p. 148) que:

"A Assinatura Digital, por chaves públicas, oferece um elevado nível de segurança, proporcionando uma presunção muito forte de que o documento onde se encontra foi criado pela pessoa que dela é titular e, assim, satisfaz o objetivo do legislador na exigência de assinatura para atribuição de valor probatório aos documentos escritos. (...) para que este processo se desenvolva é necessário que haja uma autoridade certificadora, que reunirá os dados necessários para identificar cada portador de chaves (pública e privada). O papel da autoridade certificadora é criar, ou possibilitar a criação de um par de chaves critográficas (a chave pública e a chave privada) para o usuário, além de atestar a identidade do mesmo (conferindo, minuciosamente, sua identidade física pelos meios tradicionais). A certificadora emite um "certificado" contendo a chave pública do usuário e esse certificado acompanhará os documentos eletrônicos assinados, conferindo as características essenciais da integridade e da autenticidade".

No que se refere ao nível de segurança em razão do uso da assinatura digital em documentos eletrônicos, salienta Volpi que "a assinatura digital, atualmente fundamentada na tecnologia de autenticação, possibilita uma real segurança ao seu usuário, desde que preze pela constante evolução dos algoritmos, a fim de evitar o aprimoramento pelos especialistas em decifragem, também conhecidos como criptoanalistas" (2002, p. 380-381).

Há diversas vantagens em se assinar digitalmente um documento eletrônico, dentre elas, pode-se destacar a garantia da integridade, isto é, que o documento não sofreu alterações, e também a garantia de que o documento é autêntico, ou seja, a certeza de que o documento foi elaborado pelo verdadeiro autor.

Trata-se de garantias que podem ser asseguradas com o uso da assinatura digital, pois, o documento eletrônico, na ausência desta ou de outro mecanismo similar qualquer que venha a ser elaborado, torna-se vulnerável a modificações indevidas.

Portanto, na sociedade atual, apresenta-se como fundamental o uso da assinatura digital para fornecer a garantia da integridade e autenticidade do documento em sua forma eletrônica.

Além da preocupação com a integridade e com a autenticidade do documento eletrônico, deve-se também direcionar a atenção para um outro elemento que também é de grande relevância quando se refere à segurança, trata-se da privacidade onde se deve buscar a preservação do sigilo do documento eletrônico.

A utilização da assinatura digital baseada na criptografia assimétrica protege o conteúdo dos documentos eletrônicos através da cifragem da mensagem com a chave pública do receptor, e, assim, com o uso de sua chave privada, ele poderá decifrar e ler a mensagem.

Deste modo, evita-se a falsificação e garante a autenticidade, uma vez que para realizar a assinatura é necessário ter o conhecimento da chave privada a qual por esta razão, deve ser de uso exclusivo de seu proprietário. Neste sentido, explica Peck que:

"No quesito segurança, o sistema de chaves 'públicas' e 'privadas', além de garantir o sigilo das transações ocorridas na rede, possibilita a identificação do remetente e do receptor, uma vez que é deverá saber a chave pública, correspondente à chave privada do remetente, que é a única capaz de decodificar a mensagem enviada. Sendo assim, a chave privada funciona como uma assinatura eletrônica" (2002, p. 74).

A adoção da assinatura digital com base na criptografia assimétrica, na medida em que fornece as garantias fundamentais para o estabelecimento de um ambiente seguro na celebração de negócios jurídicos em meio eletrônico, permite que diversas atividades venham a adotar o meio eletrônico por identificar nele uma alternativa para a prestação de um serviço com maior praticidade, celeridade e garantia de segurança.

A tecnologia, da mesma forma que cria novos paradigmas no âmbito do direito, também pode auxiliar a lei a solucionar os problemas decorrentes do avanço tecnológico e do desenvolvimento da sociedade, por exemplo, através da regulamentação e da utilização do certificado digital, o qual funciona como uma carteira de identidade eletrônica, permitindo assim que o cidadão seja reconhecido, podendo evitar fraudes no comércio eletrônico.

O certificado digital consiste em um documento eletrônico assinado digitalmente por uma autoridade certificadora, e que contém diversos dados sobre o emissor e o seu titular, e a sua função principal é vincular uma pessoa ou uma entidade a uma chave pública.

Desta forma, pode-se dizer que "a essência da certificação digital reside na possibilidade de garantir a autenticidade e a integridade do documento eletrônico, que é objeto caracterizador de uma transação virtual" (Kaminski, 2004, p.247).

Para adquirir um certificado digital, o cidadão interessado deve se dirigir a uma autoridade de registro, sendo identificado mediante a apresentação de documentos pessoais.

O certificado digital funciona analogicamente como uma carteira de identidade do indivíduo, desta forma, deve constar nele informações básicas, como a sua chave pública, dados pessoais, período de validade do certificado, nome da autoridade certificadora (AC) que emitiu o certificado, o número de série do certificado e a assinatura digital da AC.

III. O MODELO DE PROTEÇÃO DE PROGRAMA DE COMPUTADOR POR CERTIFICAÇÃO DIGITAL

O modelo de proteção de programa de computador por certificação digital proposto em 2001 no Centro de Ciências da Computação da Universidade Federal de Santa Catarina teve o objetivo de desenvolver uma alternativa eficaz para coibir o uso não autorizado e a distribuição ilegal de cópias de programa de computador.

Desta forma, buscou-se elaborar um modelo de proteção que tivesse propriedades capazes de quebrar o ciclo vicioso da pirataria de programa de computador, por exemplo, através da criação de mecanismos que pudessem auxiliar na tarefa de identificar o usuário infrator, responsabilizando-o pela violação aos direitos de autor de programa de computador.

A principal característica deste modelo de proteção é o fato de condicionar o registro do programa de computador ao certificado digital do usuário e assim fazer com que as cópias ilegais de programa de computador possam ser neutralizadas através da revogação do certificado de licença de uso do programa.

Para a sua viabilidade técnica, o autor do modelo de proteção adotou as providências necessárias: 1. a adoção de um padrão ASN-1 pré-definido e registrado pelo LabSEC, sob número: 1.3.6.1.4.1.7687.1.8.1. Este número representa a OID destinada ao Modelo de Proteção de Software por certificação Digital (...); 2. definição das extensões que conterão as restrições do uso destes certificados, como por exemplo, certificados destinados a licença de uso de determinado software de alguma empresa; 3. emissão de certificados digitais para teste do protótipo. Estes certificados são baseados na recomendação X.509v3 e contém as extensões necessárias para o uso do software (Rocha, 2001, p. 49).

No processo de licenciamento do programa de computador, o produtor ou a revenda funcionaria como uma autoridade de registro, ou seja, funcionaria como uma entidade responsável por verificar a veracidade dos dados informados pelo cliente, conferindo sua identidade e a autenticidade dos de seus dados.

Em seguida, há o processo de validação da licença de uso do programa de computador que é dividido em três fases.

A primeira fase tem início no momento que o usuário efetua a autenticação e aciona o programa de computador protegido, o qual verifica a existência de um certificado com extensão própria e chave privada correspondente sempre que o programa é inicializado. Em caso positivo, um desafio é gerado e depois assinado com a chave privada.

Na segunda fase, o programa de computador protegido solicita que a gerência de certificados aplique a chave pública contida no certificado para verificar a assinatura do resumo assinado na primeira parte do processo.

Na última fase do processo de validação, verifica-se se a validade do certificado não expirou; se a validade da lista de certificados revogados local não expirou; se o certificado não consta na lista de certificados revogados local ou remota.

Explica o autor que "o fato de ser o sistema operacional, através da gerência de certificados e não o software protegido, o encarregado de validar as operações ligadas ao certificado, dificulta a ação de usuários sofisticados que tentam 'quebrar' o código para retirar a proteção" (Rocha, 2001, p. 52).

Para a viabilidade do modelo de proteção, propõe o autor que seja firmado um contrato entre o usuário e a empresa de software, elegendo uma autoridade certificadora como válida entre as partes e estabelecendo ainda uma cláusula na qual os dados cadastrais do usuário serão transmitidos através da rede para confirmação das informações e averiguação de eventual existência de cópias piratas por meio do número da licença do programa de computador.

Dentre as vantagens da adoção deste modelo de proteção, além de desativar as cópias ilegais do programa de computador, desestimularia a pirataria do mesmo uma vez que seria possível identificar o usuário infrator através da sua ligação com o certificado de licença de uso do programa e, conseqüentemente, responsabilizá-lo pela violação dos direitos do autor de programa de computador.

A proteção de programa de computador por certificação digital desestimularia o usuário infrator a distribuir cópias do programa que comprou, pois "se este mesmo usuário quiser fazer uma cópia pirata e distribuí-la, necessitaria fornecer, junto com a cópia, o seu certificado e sua chave privada, o que poderia trazer inúmeras complicações para ele, pois o certificado digital está associado ao usuário através de um contrato e essa associação não pode ser negada" (Rocha, 2001, p. 37).

Por último, o modelo de proteção permitiria ainda determinar concessões de direito de uso do programa, previstas em contrato e estabelecidas pelo período de validade do certificado de licença de uso e proporcionar a personalização do programa de computador com base nas informações contidas no certificado de licença do programa.

IV. IMPLICAÇÕES LEGAIS DO MODELO DE PROTEÇÃO EM ANÁLISE

De início, uma questão que se impõe é saber se há legalidade na conduta da empresa de software que obriga o cliente a ter que adquirir um certificado digital para que possa obter a licença de uso do programa de computador.

O contrato de licença de uso de programa de computador, por se tratar de uma prestação de serviço que tem o usuário como destinatário final, caracteriza-se como uma relação de consumo, submetendo-se ao regime jurídico do Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990).

Este diploma legal assegura como um direito básico do consumidor, por exemplo, a proteção contra métodos comerciais coercitivos ou desleais, bem como práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços (art. 6º, inc. IV).

Na seção IV do Código de Defesa do Consumidor (CDC) que trata das práticas abusivas, tem-se o art. 39, caput e incisos I e V que, respectivamente, vedam ao fornecedor de produtos ou serviços, dentre outras práticas abusivas: condicionar o fornecimento de produto ou de serviço ao fornecimento de outro produto ou serviço, bem como, sem justa causa, a limites quantitativos; e exigir do consumidor vantagem manifestamente excessiva.

Desta forma, com fundamento na Lei nº 8.078/90, é possível argumentar que a empresa de software poderia estar cometendo uma prática abusiva ao obrigar o consumidor a ter que adquirir um certificado digital para que possa usufruir do serviço.

Acontece que, atualmente, há um custo para a aquisição do certificado digital do usuário junto a uma autoridade certificadora, o qual, de modo geral, é suportado pelo próprio usuário.

Trata-se de um ônus que a empresa de software criaria para o consumidor em virtude da adoção de um modelo de proteção por certificação digital o qual tem a finalidade específica de proteger a propriedade intelectual do programa de computador da empresa de software.

Assim, sob esta perspectiva, pode-se entender que, no caso em questão, há a incidência do art. 39, inc. V do Código de Defesa do Consumidor que considera como prática abusive a conduta de exigir do consumidor vantagem manifestamente excessiva.

Um segundo ponto importante é que, de modo geral, o contrato de licença de uso de programa de computador se caracteriza como um contrato de adesão, isto é, as cláusulas são estabelecidas unilateralmente pela empresa de software, restando ao consumidor a opção de aceitar ou recusar o contrato na íntegra.

Não se pode olvidar que o inciso IV do art. 51 da Lei nº 8.078/90 determina que são nulas de pleno direito, entre outras, as cláusulas contratuais relativas ao fornecimento de produtos e serviços que estabeleçam obrigações consideradas iníquas, abusivas, que coloquem o consumidor em desvantagem exagerada, ou sejam incompatíveis com a boa-fé ou a eqüidade.

Nos termos do dispositivo legal mencionado, a conduta da empresa de software de obrigar o consumidor a ter que adquirir um certificado digital pode ser considerada uma obrigação iníqua na medida em que a empresa criou uma obrigação que antes não existia, além disso, ela poderia prestar o serviço de concessão de licença de uso de programa de computador ao usuário sem que tivesse que obrigá-lo a adquirir um certificado digital na hipótese de utilizar outro tipo de proteção.

Desta forma, para afastar eventual nulidade de cláusula contratual em razão de possível caracterização de venda casada, vantagem manifestamente excessiva ou obrigação iníqua no contrato de licença de uso do programa de computador, seria aconselhável estabelecer que eventuais encargos referentes ao uso da certificado digital sejam suportados pela empresa de software.

É oportuno salientar que o modelo de proteção do programa de computador por certificação digital não foi idealizado com a finalidade de prejudicar o consumidor, mas sim de desenvolver uma forma mais eficaz de proteção contra a pirataria de programas de computador. A questão consiste, portanto, em conciliar os interesses no sentido de tornar viável o modelo de proteção por certificação digital, assegurando-se os direitos do consumidor, protegendo os direitos de autor de programa de computador e ainda contribuindo para que o Estado possa garantir o desenvolvimento nacional.

Desta forma, o primeiro passo deve ser orientar o consumidor sobre todas as peculiaridades da proteção de programa de computador por certificação digital, pois o art. 6º, inc. III do Código de Defesa do Consumidor assegura como um direito básico do consumidor a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade e preço, bem como sobre os riscos que apresentem.

O contrato de licença de uso de programa de computador protegido por certificação digital, dada sua própria natureza e peculiaridade, caracteriza-se como um contrato de adesão, desta forma, com fundamento nos art. 51, inc. IV e §1º, inc. III do CDC, é aconselhável que a empresa de software estabeleça que o foro de eleição para dirimir controvérsias oriundas do contrato seja o domicílio do consumidor.

Além de estipular a eleição do foro em benefício do consumidor, o contrato de licença de uso de programa protegido por certificação digital precisa indicar também a escolha da autoridade certificadora que será responsável pela emissão dos certificados.

Pode-se optar por utilizar certificados emitidos pela ICPBrasil os quais são dotados de presunção de veracidade, como também é possível utilizar certificados não emitidos pela ICPBrasil desde que sejam admitidos pelas partes como válidos ou aceito pela pessoa a quem for oposto o documento, conforme previsão do art. 10, §§1º e 2º da MP 2.200/01.

Trata-se de uma cláusula muito importante haja vista que a existência de controvérsia em relação à autoridade certificadora pode comprometer o funcionamento do modelo de proteção de programa de computador por certificação digital, inviabilizando, conseqüentemente, a prestação do serviço.

Na atualidade, não existe nenhuma norma legal em vigência que assegure à empresa de software ou revenda o direito de atuar como uma autoridade de registro, responsável por identificar o cliente e fornecer os dados para a autoridade certificadora, a qual pode se recusar ou aceitá-la como uma autoridade de registro ou não sem que isso constitua um ato ilícito.

Acerca destas questões envolvendo a regulamentação legal, Peck comenta que “apesar de o Brasil ser bastante avançado na área tecnológica de criptografia (...), nossa legislação está bastante atrasada na regulamentação da assinatura e da certificação virtuais” (2002, p. 87-88).

De outra forma, a empresa de software não pode se eximir de sua responsabilidade civil pelos danos que causar em virtude da adoção do modelo de proteção por certificação digital, devendo sempre respeitar os direitos do consumidor.

Nos termos do art. 51, inc. I da Lei 8.078/90, são nulas as cláusulas contratuais relativas ao fornecimento de produtos ou serviços que impossibilitem, exonerem ou atenuem a

responsabilidade do fornecedor por vícios de qualquer natureza dos produtos e serviços ou impliquem renúncia ou disposição de direitos.

O art. 43, §2º do Código de Defesa do Consumidor determina que "a abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele".

Em decorrência do disposto nesta norma, a empresa de software não pode incluir o certificado de licença de uso do programa de computador do usuário na lista de certificados revogados sem antes comunicar o consumidor por escrito, pois o certificado digital de licença de uso do programa nada mais é do que um documento eletrônico que contém dados pessoais do usuário.

A inclusão do certificado de licença de uso do programa de computador do usuário na lista de certificados revogados pode trazer transtornos para o consumidor, impedindo-o de ter acesso ao programa de computador, pois o programa, ao estar conectado à internet e realizar a consulta à lista de certifivados revogados, não mais funcionará, inviabilizando o acesso ao mesmo em razão da revogação do certificado.

Desta forma, é aconselhável que o contrato de licença de uso de programa de computador protegido por certificação digital estabeleça as hipóteses em que a empresa de software poderá incluir o certificado de licença na lista de certificados revogados, devendo, em todo o caso, avisar previamente o consumidor por escrito para evitar a sua responsabilização pelos danos morais decorrentes da inobservância aos preceitos legais.

Em razão da peculiaridade do contrato de licença e do modelo de proteção por certificação digital, o contrato celebrado entre as partes precisa observar o respeito às normas do Código de Defesa do Consumidor para que tenha viabilidade perante o ordenamento jurídico brasileiro.

Além de consagrar a defesa do consumidor como uma garantia fundamental do cidadão no art. 5º, inc. XXXII, a Constituição Federal também assegura o direito da propriedade intelectual do autor no art. 5º, inc. XXVII e ainda consagra o direito à privacidade no art. 5º, inc. X e XII.

A Carta Magna tem como um de seus objetivos fundamentais garantir o desenvolvimento nacional e esta finalidade se apresenta incompatível com a pirataria.

Entretanto, se, de um lado, existe o objetivo de proteger os direitos do autor de programa de computador e garantir o desenvolvimento nacional, por outro, existe o direito fundamental à privacidade.

A proteção da privacidade dos dados pessoais do cidadão transmitidos através da rede é fundamental para evitar, por exemplo, a ocorrência de danos devido ao conhecimento de informações as quais deveriam ser mantidas em sigilo.

Desta forma, para que o modelo de proteção proposto por Rocha esteja em harmonia com o direito à privacidade, deve-se assegurar ao usuário o direito de saber exatamente o conteúdo dos seus dados pessoais que estejam sendo enviados pela rede e a faculdade de interferir neste processo.

No modelo de proteção em análise, observa-se que algumas operações podem acontecer sem a interferência do usuário, de forma imperceptível e sem a sua anuência na transmissão de tais dados. Isto acontece, por exemplo, no processo de validação da licença de uso do programa de computador, ao verificar a validade do certificado digital.

Para evitar este problema, o modelo de proteção por certificação digital deve permitir que o usuário tenha conhecimento de todos os dados que serão transmitidos através da rede e que lhe seja assegurada a faculdade de interferir neste processo, possibilitando-o impedir, por exemplo, a verificação automática que consulta se o certificado não consta na lista de certificados revogados local.

Por conseqüência, para uma maior segurança juridical para as empresas de software, seria interessante uma cláusula contratual que estabeleça que na hipótese de o usuário se recusar a fornecer as informações essenciais para a validação do certificado digital, o processo de validação do programa será interrompido, de forma que o usuário não terá acesso ao programa, podendo implicar na rescisão do contrato de licença.

V. CONCLUSÃO

A tecnologia pode contribuir para proporcionar uma maior eficácia da lei, na medida em que cria mecanismos técnicos que podem auxiliar na tarefa de coibir a prática de comportamentos proibidos pela legislação vigente.

Para que seja viável o uso da certificação digital para proteger os direitos do autor de programa de computador, é necessário que o contrato firmado entre as partes observe o respeito aos direitos e garantias fundamentais do cidadão.

Desta forma, sugere-se que os encargos com a certificação digital sejam suportados pela empresa de software, pois, de outro modo, ela poderia estar cometendo uma prática abusiva ao obrigar o consumidor a ter que adquirir um certificado digital, junto a uma autoridade certificadora, para que possa usufruir do serviço.

É oportuno enfatizar que o consumidor tem direito à informação adequada e suficiente sobre os riscos que o negógico jurídico apresenta, portanto, a empresa de software tem a obrigação de esclarecê-lo sobre o funcionamento do programa de computador e das peculiaridades do modelo de proteção em todos os seus aspectos.

Além disso, por observância ao direito à privacidade do cidadão, o programa de computador protegido somente poderá transmitir as informações essenciais para o funcionamento do processo de validação da licença de software através da rede quando houver prévia concordância por parte do usuário, facultando-lhe a possibilidade de cancelar o envio das mesmas.

Muitos consumidores não lêem atentamente os contratos, principalmente em se tratando de contratos eletrônicos. Portanto, seria aconselhável criar uma interface junto ao modelo de proteção que permita ao consumidor tomar

conhecimento de todas e quaisquer informações e dados de seu computador que estejam sendo transmitidos através da rede, possibilitando ao mesmo interferir no envio de tais informações, mesmo que a recusa do consumidor implique no não funcionamento do programa.

Entretanto, verificou-se que existem dados que são essenciais para que este modelo de proteção possa atingir a sua finalidade que se referem, por exemplo, às informações acerca da data de validade do certificado para verificar se o certificado não expirou, da validade da lista de certificados revogados local e da verificação se o certificado não consta na lista de certificados revogados local.

Para resolver esta questão, propõe-se uma cláusula contratual que estabeleça que na hipótese de o usuário se recusar a fornecer as informações essenciais para a validação do certificado digital, o processo de validação do programa de computador será interrompido, de forma que o usuário não terá acesso ao programa.

Isto poderá implicar na rescisão do contrato de licença de uso do programa e, neste caso, não se caracteriza defeito ou vício do serviço haja vista que o consumidor, tendo conhecimento das peculiaridades de modelo de proteção, deu causa ao seu não funcionamento por se recusar a fornecer os dados necessários ao sistema de proteção.

De modo geral, o maior problema envolvendo a privacidade dos usuários é o fato de que as empresas de software comercializam licenças de uso de programas de computador que apresentam código-fonte fechado e protegidos pelo sigilo, de forma que podem conter neles códigos maliciosos ou operações que violem o direito à privacidade do usuário.

As empresas de software têm o dever de informar o consumidor sobre as propriedades e características de seus programas, inclusive no que concerne aos riscos que podem apresentar.

A certificação digital pode contribuir para a proteção dos direitos de autor de programa de computador através do modelo de proteção por certificação digital proposto por Rocha, desde que sejam assegurados os direitos do consumidor e a privacidade de seus dados pessoais.

Em último caso, tendo em vista a peculiaridade da proteção de programa de computador por certificação digital e suas possíveis implicações legais bem como o fato de que as normas que tratam da matéria foram instituídas através de uma medida provisória de forma muito precária, seria interessante a elaboração de uma lei específica para regulamentar o assunto de forma mais aprofundada.

REFERÊNCIAS

[1] R. O. Blum. A internet e os tribunais. In: R. Demócrito Filho (Org.). "Direito da Informática: temas polêmicos". Bauru: Edipro, 2002. pp. 145-150.

[2] D. Brown, "Fortaleza Digital". Trad. de Carlos Irineu da Costa. Rio de

[3] Janeiro: Sextante, 2005. 331 p.

[4] G. T. Corrêa. "Aspectos jurídicos da internet". São Paulo: Saraiva, 2000. 135 p.

[5] F. E. Z. Glitz. O contrato internacional celebrado pela troca de mensagens eletrônicas: a perspectiva do direito brasileiro. In: L. O. Pimentel (Org.). "Direito Internacional e da Integração". Florianópolis: Fundação Boiteux, 2003. 1071 p.

[6] ITI. Instituto Nacional de Tecnologia da Informação. Disponível em: <http://www.iti.org.br>. Acesso em: 17 de dez. 2005.

[7] O. Kaminski (Org.). "Internet legal: O Direito na Tecnologia da Informação". Curitiba: Juruá, 2003. 291 p.

[8] M. E. Leite. Comércio eletrônico nova modalidade de comércio internacional. In: L. O. Pimentel (Org.). "Direito Internacional e da Integração". Florianópolis: Fundação Boiteux, 2003. 1071 p.

[9] F. Noronha. "Direito das Obrigações" v.1. São Paulo: Saraiva, 2003. 698 p.

[10] P. Peck. "Direito Digital" São Paulo: Saraiva, 2002. 290 p.

[11] M. C. Pereira. "Direito à Intimidade na Internet". Curitiba: Juruá, 2003. 279p.

[12] D. Reinaldo Filho (Org.). "Direito da Informática: temas polêmicos". Bauru: Edipro, 2002. 432 p.

[13] J. L. F. Rocha. "Proteção de Software por Certificação Digital". Dissertação de Mestrado. Universidade Federal de Santa Catarina. Florianópolis, 2001. 76p.

[14] J. A. da Silva. "Curso de Direito Constitucional positivo". 22.ed. rev. e atual. São Paulo: Malheiros, 2003. 878 p.

[15] N. Silveira. "A propriedade intelectual e as novas leis autorais". São Paulo: Saraiva, 1998. 345 p.

[16] L. H. Ventura. "Comércio e contratos eletrônicos". Bauru (SP): Edipro, 2001. 134 p.

[17] C. S. M. Vianna. Software e privacidade: uma defesa do código-fonte aberto na preservação do direito constitucional à vida privada. In: "Jus Navigandi", Teresina, ano 6, n. 57, jul. 2002. Disponível em:<http://jus2.uol.com.br/doutrina/texto.asp?id=2931>. Acesso em: 08 jan. 2006.

[18] M. M. Volpi. Assinatura digital e sua regulamentação no Brasil. In: D. Reinaldo Filho (Org.). "Direito da Informática: temas polêmicos". Bauru: Edipro, 2002. pp. 367-382.

[19] M. Wachowicz. "Propriedade intelectual do software & revolução da tecnologia da informação". Curitiba: Juruá, 2004b. 287 p.

Hélio S. Ramos Júnior é estudante de Direito da Universidade Federal de Santa Catarina (UFSC), foi monitor da Disciplina Informática Jurídica, foi Bolsista de Iniciação Científica pelo CNPq, Conciliador do Juizado Especial Criminal do Fórum Distrital do Norte da Ilha da Comarca da Capital (SC), Pesquisador do Laboratório de Informática Jurídica do Centro de Ciências Jurídicas, atualmente trabalha como estagiário no Centro de Apoio Operacional do Consumidor - Ministério Público de Santa Catarina. É autor e co-autor das seguintes obras: "Considerações legais sobre a privacidade no espaço cibernético" (2003), "Segurança na análise de crédito: um direito do cidadão" (2004), "Os atores sociais e a cidadania na sociedade da informação e do conhecimento" (2004), "A tutela jurídica do consumidor e a publicidade abusiva em rede" (2005), "BuscaLegis: Uma Biblioteca Jurídica Virtual" (2005), "O ato administrativo eletrônico sob a ótica do princípio da eficiência" (2005), "Perspectivas para a teleadministração no Brasil: sistemas inteligentes e software livre na Administração Pública" (2006). E-mail: helio@grad.ufsc.br.

MODELO HÍBRIDO BASEADO EM REDES NEURAIS E SISTEMAS ESPECIALISTAS PARA DETECÇÕO DE INTRUSOS EM REDES DE COMPUTADORES TCP/IP

M.Sc. André Calazans Barreira , Dr. Rogério Alvarenga[2] e M.Sc Jerônimo Jardim
andre@calazans.net[1], rogerio@ucb.br[2] , j2odias@gmail.com[3]

Resumo - No universo da Segurança da Informação, para se criar e manter um "estado" seguro, aspectos como integridade, confidencialidade e disponibilidade devem ser garantidos. Nesse contexto, os Sistemas de Detecção de Intrusão - SDI para computadores ou rede de computadores, são mecanismos importantes para percepção de ações delituosas que visam ao comprometimento de, pelo menos, um dos três, senão os três aspectos citados acima. Assim, detectar o intruso, de maneira efetiva, pode ser o diferencial para a percepção e diagnose de um ataque. Portanto, eventos avaliados como falsos alarmes (falsos positivos), interpretações incorretas de logs e intrusões percebidas e não registradas por esses Sistemas (falsos negativos) devem ser minimizados. Este artigo apresenta um modelo que busca, por meio através da combinação de técnicas de Sistemas Inteligentes – Redes Neurais Artificiais e Sistemas Especialistas atingir este objetivo.

I. INTRODUÇÕO

SÃO inúmeros os desafios impostos pela globalização dos mercados, principalmente aqueles relacionados a questões tecnológicas. Atualmente não basta a simples conexão a uma grande rede de serviços, é preciso que tal conexão seja rápida e que minimamente esteja disponível. Não é difícil imaginar que a não realização de uma transação, seja ela comercial ou financeira, em tempo hábil, possa comprometer a sobrevivência de uma empresa.

Nesse universo, percebe-se o avanço na construção e manutenção de uma infra-estrutura de rede de computadores e telecomunicações capaz de prover a demanda de serviços criada.

Com a crescente utilização desses serviços, outros fatores foram agregados a essa infra-estrutura, como por exemplo, a confidencialidade. Para alguns, não basta a integridade da conexão e nem sua disponibilidade se o caráter confidencial não estiver presente. É nesse tripé: integridade, disponibilidade e confidencialidade que está constituído o contexto da Segurança da Informação [1].

Visualizar a segurança, como um estado obtido através da implementação e gestão de diversas práticas que também assegurem esse tripé é fundamental para a percepção de seu aspecto dinâmico e contínuo.

Políticas de segurança, Planos de Continuidade de Negócios, Controle de acessos – físicos e lógicos, a utilização de *Firewalls*, Antivírus, Criptografia, Sistemas de Detecção de Intrusão, são alguns elementos que, uma vez implantados nas organizações, podem prover maior grau de segurança.

Cada um desses instrumentos traz consigo suas peculiaridades, o que deve ser levado em consideração quando da sua implementação. Por exemplo: a criptografia utilizada por uma corporação não pode ser "pesada" a ponto de comprometer o tráfego dos dados, inviabilizando assim sua utilização; Planos de Continuidade de Negócio devem contemplar situações de recuperação de desastres, sob pena de não cumprirem sua finalidade, ou ainda, Sistemas de Detecção de Intrusos, cujos "registros" apontem para atitudes não intrusivas, que não registrem as intrusões ou ainda que a induzam falsas interpretações, podem não ser de grande utilidade para o ambiente da segurança corporativa.

Dentro desse escopo, tal modelo espera contribuir com a apresentação e a implementação de um mecanismo híbrido capaz de combinar o que se conhece por técnicas de detecção de intrusão por conhecimento e por comportamento, utilizando técnicas de Inteligência Artificial (Sistemas Inteligentes), como Redes Neurais Artificiais – RNA e Sistemas Especialistas – SE.

II. SISTEMAS DE DETECÇÕO DE INTRUSÕO - SDI

Para *Rebeca e Mell* [2], "intrusão é qualquer tentativa de comprometer a confidencialidade, integridade e disponibilidade de um sistema ou a tentativa de burlar os mecanismos de segurança de um servidor ou da rede." A intrusão pode ter origem em um atacante acessando o sistema via Internet, em um usuário autorizado que tente ganhar privilégios adicionais ou em usuários que façam mau uso dos privilégios que possuem.

Rebeca e Mell [2] definem SDIs como "sistemas de software ou hardware, que automatizam o processo de monitorar eventos ocorridos em uma rede de

computadores, analisando-os em busca de sinais de violação da segurança."

Assim, de acordo com Barreira e Guedes [3], "Sistemas de detecção de intrusão (SDI) têm a função de emitir alertas na ocorrência ou iminência de um ataque. Eles automatizam o processo de monitorar eventos que ocorrem em uma máquina ou em uma rede e analisam estes eventos em busca de sinais de que há falha na segurança."

Seja qual for o SDI, ele conterá, de forma genérica, os seguintes componentes:

a) gerador de eventos (E-box) – é a parte responsável por capturar eventos no meio externo ao SDI e padronizar os dados obtidos. A filtragem de registros de auditoria e a captura de pacotes são exemplos de geração de eventos;

b) analisador de eventos (A-box) – recebe os dados do gerador de eventos e busca padrões que caracterizem um ataque;

c) base de dados de eventos (D-box) – armazena os eventos em um arquivo para análise futura [4].

A idéia inicial para um Sistema de Detecção de Intrusos está presente no documento denominado *Computer Security Threat Monitoring and Surveilance,* que data da década de 80 que trata-se basicamente de um relatório com o propósito de melhorar a segurança dos computadores, em determinado ambiente, sob o foco da capacidade de se vigiar sistemas [5].

Em 1983, no laboratório da SRI Internacional, surge o primeiro protótipo de um SDI, à época, denominado IDES – *Intrusion Detection Expert System,* porém é entre 1984 e 1987, através dos trabalhos de *Dorothy E. Denning* e *P. Neumann,* que um modelo de IDES é proposto e desenvolvido. [6]. O modelo propunha duas técnicas de detecção de intrusão: uma delas baseada em regras previamente definidas, e a outra baseada na verificação de perfis. Nesse momento, nasce o que, mais a frente, define-se como modelos baseados em conhecimento e comportamento respectivamente [13].

Logo após, surge a idéia do SDI Distribuído que culmina com a proposta do primeiro SDI para rede de computadores, o que dá origem à denominação NSDI baseado em rede. Assim o NSM – *Network Security Monitor* - tornou-se inovador, à época, pois abordava a possibilidade de se monitorar um segmento de rede Ethernet [12].

As pesquisas mais recentes apontam, basicamente, para dois caminhos: um deles é a criação de novos modelos, isto é, elementos constitutivos de um SDI são alterados ou têm sua dinâmica modificada, buscando o processo de melhoria, e o outro é a tentativa de se estabelecer padrões, através da análise de perfis refinados que representam o comportamento do usuário, dando, assim, continuidade evolutiva ao proposto lá na década de 80.

A. Classificação de um SDI

Bace e Mell [2] e Weber, Campelo [4], classificam SDI's segundo quatro critérios:

a) Método de Detecção: a detecção de um ataque pode ser baseada em comportamento ou em conhecimento. No primeiro caso, a ferramenta SDI traça um perfil do comportamento considerado normal e alerta quando algo fora deste padrão ocorrer. No segundo caso, o SDI possui uma base de assinaturas, semelhante aos programas antivírus, que contém os padrões de ações de intrusão conhecidos. Ele, então, compara o tráfego monitorado com estes padrões e alerta quando encontra alguma correspondência;

b) Arquitetura: os sistemas de detecção podem ser baseados em rede, quando monitoram o tráfego da rede, mas ignoram que se passa em cada máquina internamente; em host, quando monitoram as máquinas, mas ignoram o que se passa nos elementos de rede ou em outras máquinas, ou híbridos;

c) Comportamento Pós-detecção: pode ser ativo ou passivo;

d) Freqüência de Uso: um SDI pode ser destinado a monitoramento contínuo ou à análise periódica.

III. O USO DE TÉCNICAS DE SISTEMAS INTELIGENTES NA DETECÇÕO DE INTRUSÕO

No início da década de 90, surgiram os primeiros trabalhos que utilizam RNAs como instrumento de percepção da atividade intrusiva. Em 1992, um modelo denominado IDES – *Intrusion Detection Expert System* - é proposto, tendo em sua constituição elementos de RNA's e SE's, problemas com a escalabilidade do sistema e o treinamento do elemento de RNA, além dos testes terem sido realizados somente com os eventos de *logon* e *logout* são características desse modelo [7].

Cannady [8] apresenta resultados sobre a utilidade de uma Rede Neural Artificial, do tipo, MLP – Multi Layer Perceptron no reconhecimento de ataques, como *SYNFlood, SATAN test* e *ISS Scan test*, Satade utilização de RNAs, do tipo MLP – *Multi Layer Perceptron* para a detecção de intrusão, porém aponta problemas com a diversidade de comandos no campo de dados de um datagrama do IP – *Internet Protocol.*

Ainda utilizando RNA e no mesmo ano, outro trabalho é apresentado onde resultados de um NNID – *Neural Network Intrusion Detector* - são apresentados, cujo funcionamento se dá através da percepção das ações intrusivas, baseando-se em perfis que representam a ação de 100 comandos utilizados pelo usuário.

Apresentou taxa de acerto em 93% nos testes com uma taxa de 7% de falso positivo [9].

Em 2001 e 2002 outros trabalhos com a utilização de RNA's são apresentados e não fogem dos, até então, propostos, à exceção da inovação com a utilização do algoritmo de LVQ - *Learning Vector Quantization* [10].

Já em 2003, a utilização de SVM's – *Support Vector Machines* é apresentada e validada sob a coleção de dados intrusivos do DARPA dos EUA - *Defense Advanced Research Projects Agency* - ratificando como resultado a prática da técnica para a utilização em ferramenta de detecção de intrusão em tempo real [11].

IV. O MODELO PROPOSTO

Diz-se que o modelo proposto é híbrido por duas razões: a primeira por combinar duas técnicas de Sistemas Inteligentes – Redes Neurais Artificiais e Sistemas Especialistas; e a segunda por também, combinar dois métodos diferenciados de detecção de intrusão – aqueles baseados em comportamento e em conhecimento. Tal relação pode ser estabelecida de forma direta, isto é, a submissão à RNA está para a detecção em comportamento, assim como a apreciação pelo Sistema Especialista está para a detecção baseada em conhecimento.

Para a aplicação e implementação do modelo foi desenvolvido uma nova ferramenta de detecção, que satisfaz aos requisitos apresentados no item 2 desse artigo, denominada *Newnids*.

Está inscrita em linguagem C e para o Sistema Operacional LINUX.

Assim, a proposta é a seguinte: perceber o tráfego entrante em uma rede de computadores, que usa tecnologia ETHERNET e está baseada em TCP/IP, submetê-lo ao parecer de uma RNA do tipo MLP, cujo resultado será submetido ou não a um Sistema Especialista (ambos formam a *Engine*) o que findará na diagnose se ação é ou não intrusiva.

Pode-se resumir em etapas o fluxo dos pacotes através do modelo:

1) a captura dos pacotes;
2) a decodificação dos pacotes e conseqüente obtenção dos valores que serão submetidos à *Engine* de detecção;
3) O parecer da RNA e, em caso de dúvida, da ação intrusiva, subseqüente submissão ao Sistema Especialista;
4) Registro do diagnóstico, seja ela da RNA ou do SE.

A figura 1 apresenta o modelo.

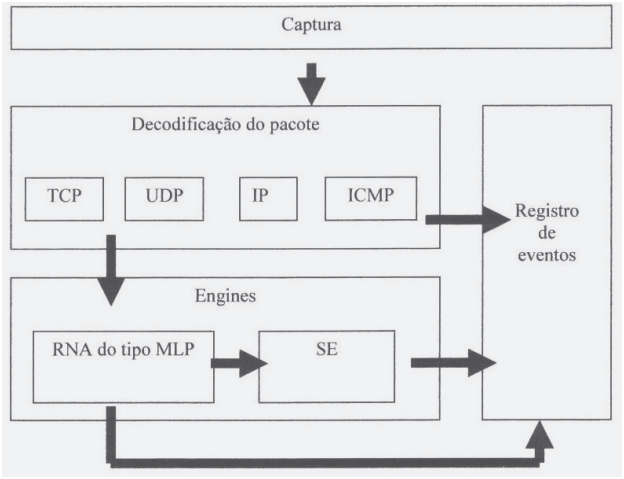


Figura 1 – Representação do fluxo da informação através da ferramenta Newnids.

A captura está baseada na biblioteca *libpcap* sendo similar a outras ferramentas de coleta de tráfego, como TCPDUMP e ETHEREAL, podendo impor a interface de rede à operação em modo promíscuo.

O processo de decodificação obedece ao padrão definido em RFC – *Request for Comment* - para cada protocolo. Desta forma, é possível extrair toda a informação protocolar existente no pacote.

A. Características da RNA utilizada

Para a técnica de detecção por comportamento, foi utilizada uma RNA face a sua capacidade de abstração.

Na detecção por comportamento, o maior desafio é a diminuição dos eventos falsos positivos e as falsas interpretações, e uma grande vantagem está na possibilidade de identificação de novos padrões de ataque.

A RNA é do tipo MLP - *Multi Layer Perceptron* com 16 neurônios na camada de entrada, 7 na camada intermediária e 1 na saída. O neurônio da saída é o responsável pela diagnose, e seu valor pode variar entre 0,000000 e 1,00. Se for menor que 0,3, o pacote de dados é considerado normal. Se estiver entre 0,3000000 e 0,600000, o pacote é considerado suspeito e então precisa, ainda, do parecer do Sistema Especialista para o posicionamento final. E por fim, se ele é maior que 0,600000 é considerado intrusivo.

Para o processo de treinamento foi utilizada a estrutura do software EasyNN, atendendo ao fluxo proposto pela figura 2, tendo a base de registros sido extraída de ambiente criado exclusivamente para a captura de pacotes considerados intrusivos a partir da utilização de algumas técnicas de varredura de portas e *http evasion e insertion*.

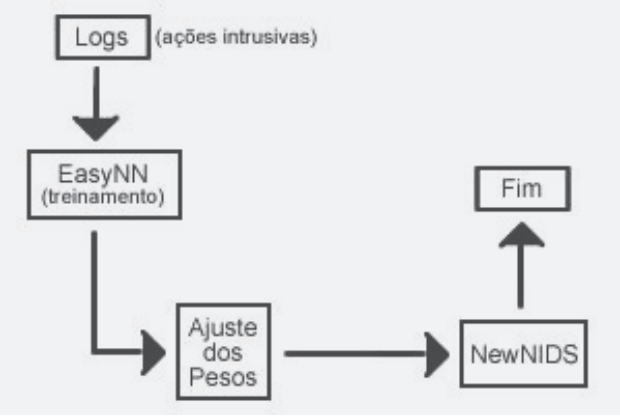


Figura 2 – O processo de treinamento e incorporação dos pesos ao código da ferramenta Newnids

A figura 3 apresenta a curva de aprendizado pertinente a RNA treinada, extraída do software EasyNN.

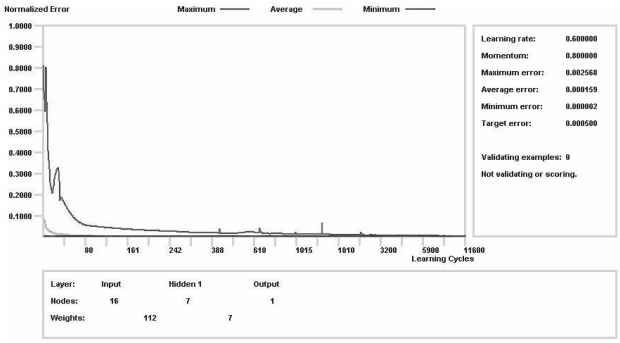


Figura 3 – Curva de aprendizado da RNA gerada pelo EasyNN.

Em qualquer uma dessas avaliações, pode-se efetuar o registro do resultado em logs, onde, através do Newnids, há a indicação de qual dos mecanismos de detecção foi o responsável pelo diagnóstico e o que o levou a tal resultado.

A figura 3 apresenta um registro de parecer da RNA para um pacote normal (RNA OUT: 0.001894).

```
ENGINE RNA: PROTO: 6 FLAGS: 18 IP
HLen:20   IPS:   200.152.161.128:80
IPD: 192.168.0.186:32784 Data Len:
0
ASCII SIG: 10 ICMP CODE: 0 RNA OUT:
0.001894
```

Figura 3 – Exemplo de parecer dado pela RNA.

A figura 4 apresenta a RNA idealizada, onde os neurônios de entrada são representados pelos seguintes campos extraídos de pacote de dados:

a) Protocolo correspondente, na RNA = *proto*. Para o protocolo TCP, o campo receberá valor 06, para o protocolo UDP, 17, e para o ICMP 01, por definição de padrão;

b) Endereço IP de origem, na RNA = *ips1, ips2, ips3 e ips4.* Recebem seus valores obedecendo a uma regra específica;

c) Endereço IP de destino, na RNA = *ipd1, ipd2, ipd3 e ipd4.* Recebem seus valores obedecendo a mesma regra para o IP de origem;

d) Porta TCP de origem, na RNA = *s_port*; recebe qualquer valor entre 0 e 65535, por definição de padrão, dependendo do serviço que se está oferecendo;

e) Porta TCP de destino, na RNA = *d_port*, obedece ao mesmo critério da porta de origem;

f) Flags TCP, na RNA = *flags*;

g) Tamanho do cabeçalho TCP, na RNA = *h_len*;

h) Mensagem ICMP, na RNA = *icmp_cod*;

i) Assinatura dos dados, na RNA = *d_sig*;

j) Tamanho do datagrama, na RNA = *d_len*.

Os endereços IP de origem e destino do pacote estão representados na RNA de forma diferenciada face a problemas de conversão. Assim, obedeceram à seguinte regra:

a) Obtêm-se os valores em *network byte order* para arquiteturas *little endian*, ou seja o bit menos significativo vem primeiro;

b) Esse valor é convertido usando-se a função *nthol()* para um inteiro longo e sem sinal de 32 bits;

c) O resultado é submetido à função *inet_ntoa()* que gera, como saída, o número IP em notação de ponto, que é novamente convertido em um inteiro *long* usando a função *inet_addr()*;

d) Para finalizar, são realizadas 4 operações de deslocamento de bits, de onde se obtém 4 partes numéricas, representativas para cada octeto e que, na RNA, estão identificadas como *ips1, ips2, ips3 e ips4* para o número IP de origem e *ipd1, ipd2, ipd3 e ipd4* para o número IP de destino.

Outro campo que precisou de tratamento diferenciado foi o *payload*, isto é, aquele que contém os dados do pacote. Para este, foi criado um *checkum* através da fórmula: (anterior * sua_posição) + (atual * sua_posição) + (posterior * sua_posição), sendo esta aplicada a cada byte do vetor responsável deste campo. Esse resultado esta armazenado na RNA sob o nome de *d_sig*.

B. O Sistema Especialista

Ferramentas de detecção de intrusos baseadas em conhecimento utilizam-se de bases de regras para a efetiva percepção da ação delituosa. Constroem essa base de regras a partir do conhecimento e interpretação

de ataques registrados à rede de computadores ou *hosts*. Assim, aquilo que já é conhecido como intrusivo é consignado ao conjunto de regras, o que possibilita a criação de uma base de conhecimento.

A desvantagem nesse tipo de detecção está no caráter estático das regras, o que impede, por exemplo, a compreensão de um novo padrão de ataque, porém o número de falsos positivos tem se demonstrado menor.

No caso especifico do modelo proposto, utiliza-se um Sistema Especialista baseado em regras. Tais regras podem ser originadas, por exemplo, pelas informações contidas nas regras da ferramenta SNORT, disponível em *www.snort.org*, ou ainda, contemplar especificidades definidas pelo usuário.

Elas estão em um arquivo próprio que é consultado e carregado quando da inicialização da ferramenta.

A tabela 1 apresenta o formato de uma regra.

TABELA I
Formato de uma regra da ferramenta Newnids

	Campo	Valor
Se	Protocolo	
E	Número Ip do Servidor	
E	Número da porta TCP	
E	Mensagem a ser gravada no evento	
E	Fluxo do pacote	
E	Conteúdo procurado no *payload*	
Então	Categorização do ataque	

V. LIMITAÇÕES IMPOSTAS AO MODELO

Não foram focadas, no modelo proposto, dificuldades já relacionadas na literatura, como ”inibidoras” da efetividade de um SDI, tais como:

a) A percepção e captura em redes de alta velocidade;

b) A questão do tráfego criptografado;

c) O posicionamento de um SDI;

d) Características de desempenho da ferramenta de SDI em rede.

Backbones que utilizem tecnologias de rede do tipo ATM e FDDI também não foram contemplados.

VI. AS VANTAGENS DO MODELO

Em um primeiro momento, observam-se as seguintes vantagens na aplicação do modelo:

a) A combinação da utilização dos dois métodos de detecção de intrusos, permite maximizar os acertos e minimizar os erros, equação essa extremamente importante quando se fala em percepção da atividade intrusiva;

b) A possibilidade de se permitir um caráter exclusivo à aplicação, isto é, o usuário familiarizado com as variáveis envolvidas pode retreinar a RNA concebida e criar suas próprias regras, personificando, assim, a ferramenta;

c) A possibilidade de se minimizar a intervenção humana na gestão diária de um SDI.

VII. TRABALHOS FUTUROS

De pronto, quatro iniciativas poderiam contribuir para a continuidade e melhoria do modelo apresentado:

a) A inclusão de análise por estado, isto é, a percepção de todo um *handshake* em uma conexão TCP como um conjunto, já que a proposta inicial contempla a análise de pacote a pacote;

b) A criação de RNA diferentes e independentes para cada protocolo pode aumentar o refinamento da ferramenta sem impactar na performance de análise do tráfego;

c) A substituição da RNA do tipo MLP por uma do tipo ART e / ou KOHONEN, alcançando, assim os benefícios impostos pelas redes do tipo *SOM's – Self Organize Maps*;

d) A não submissão ao elemento neural do endereçamento IP;

e) O desenvolvimento em modo ”kernel use” aproveitando as tecnologias existentes para esse modo naquilo que diz respeito à análise do tráfego em redes de alta velocidade, bem como a implementação da análise de estado de uma conexão TCP.

VIII. CONCLUSÕO

O modelo foi avaliado sob dois aspectos. O primeiro, quanto à atividade intrusiva, e o outro, quanto à percepção do tráfego normal. Para a percepção da atividade intrusiva, foram utilizadas técnicas de varredura de portas e http *evasion* e *insertion* onde se obteve 100% de detecção, à exceção dos pacotes UDP que, por definição, foram dirigidos diretamente ao SE, inexistindo, assim, falsos negativos. Já a submissão à atividade normal visava basicamente à detecção da presença de falsos positivos, cujo resultado aproximou-se de 1,02% médio dos pacotes, valor considerado bastante bom diante do aferido médio para técnicas de

http *evasion* e *insertion*, através de outras ferramentas, como o SNORT (33,35%) e Firestorm (42,14%) e para a técnica de varredura de portas 4,71% para o SNORT e 12,93 para o Firestorm[14].

Evidenciou-se que o modelo proposto utiliza o potencial de generalização, obtido naturalmente pela rede neural durante a aprendizagem dos padrões de ataques já classificados, aumentando a eficácia da rede para técnicas derivadas das formas de ataque já conhecidas.

Quanto aos incertos (assim classificados pela engine RNA), o sistema especialista atua como um certificador, identificando, através da sua base de conhecimento, a qualidade dos dados, buscando reduzir incertezas.

Portanto, a combinação de técnicas de detecção de intrusão com representação neural e simbólica pode constituir maior qualidade no processo de detecção de intrusão.

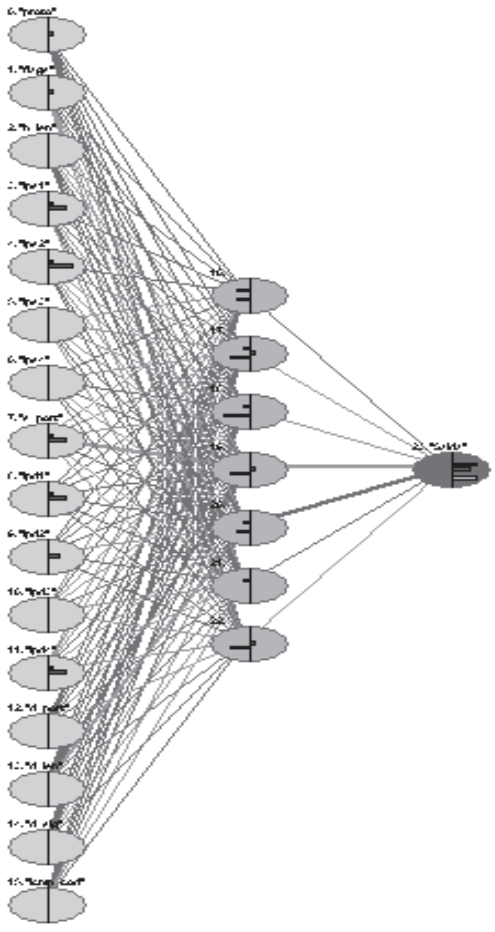


Figura 4 – A Rede Neural Artificial do Newnids

IX. REFERÁNCIAS BIBLIOGRÁFICAS

[1] NBR ISO/IEC 17799. Tecnologia da Informação – Código de prática para a gestão da segurança da informação. ABNT, 2001.

[2] BACE, Rebecca; MELL, Peter. Intrusion Detection Systems. NIST, 2001. (Disponível em http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf - acessado em 16.11.2003.)

[3] BARREIRA, André; GUEDES, William. Estudo de Caso de Implementação e Manutenção de SDI de Domínio Público. 2001. Monografia (Pós-Graduação Lato Sensu em Segurança de Redes de Computadores), UCB, Brasília-DF.

[4] BARREIRA, André; Dissertação de Mestrado. Modelo Híbrido Baseado em Sistemas Inteligentes para Detecção de Intrusos em Redes TCP/IP. Pós-Graduação Strictu Sensu em Gestão do Conhecimento e da Tecnologia da Informação; Orientação : Rogério Alvarenga, DSc; UCB, Brasília - DF, 2006.

[5] ANDERSON, James P. Co. Computer Security Threat Monitoring and Surveillance. 1980. Disponível em: http://csrc.nist.gov/publications/history/ande80.pdf - consultado em 15/01/04.

[6] SRI. Intrusion Detection – History. 2002. Disponível em http://www.sdl.sri.com/programs/intrusion/history.html - consultado em 17/01/04

[7] DEBAR, H., BECKER, M., e SIBONI, D. A Neural Network Component for a Intrusion Detection System. In Proceedings of the IEEE Computer Society Symposium, Research in Security and Privacy. 1992. pp 240-250.

[8] CANNADY, J. Artificial Neural Networks for Misuse Detection. 1998. Disponível em http://citeseer.ist.psu.edu/cannady98artificial.html – consultado em 17/01/2004.

[9] RYAN, Jake; LIN, Meng-Jang; MIKKULAINEN, Risto. Intrusion Detection with Neural Networks. 1998. Disponível em http://citeseer.ist.psu.edu/ryan98intrusion.html - consultado em 30/03/04

[10] MARLIN, Jack; RAGSDALE, Daniel; SURDU, John. A Hybrid Approach to the Profile Creation and Intrusion Detection. IEEE Proceedings of the DARPA Information Survivability Conference and Exposition, 2001.

[11] MUKKAMALA, Srinivas; SUNG, Andrew. Feature Ranking and Selection for Intrusion Detection Systems Using Support Vector. 2003. Disponível em http://citeseer.ist.psu.edu/583136.html - consultado em 22.03.04.

[12] HEBERLEIN, Tood et al. A Network Security Monitor. IEEE Computer Society. Proceedings of the IEEE Computer Society Symposium, Research in Security and Privacy.1990, pp. 296-303, pp. 296-303.

[13] DENNING, Dorothy E. An Intrusion-Detection Model. IEEE Transactions on Software Engineering, vol. SE-13, nº 2. 1987, 222-232. Disponível em: http://www.cs.georgetown.edu/~denning/infosec/SDI-model.rtf - consultado em 17/01/04

[14] FAGUNDES, Leonardo. Metodologia para avaliação de sistemas de detecção de intrusão. 2002. Monografia (Bacharelado em Informática), Universidade do Vale do Rio dos Sinos, São Leopoldo-Brasil.

[15] WEBER, Raul Fernando; CAMPELLO, Rafael Saldanha. Sistemas de Detecção de Intrusão. Instituto de Informática – UFRGS, 2001 (Disponível em http://www.inf.ufrgs.br/~gseg/producao/minicurso-SDI-sbrc-2001.pdf - consultado em 16.11.2003).

Recovering previous versions of Microsoft Word documents

Murilo Tito Pereira and Alexandre Cardoso de Barros
Brazilian Federal Police
{murilo.mtp , alexandre.acb}@dpf.gov.br

Abstract— The Microsoft Word is one of the most utilized editors in the world. Most of the time, the analysis of a Microsoft Word document is just simple as verifying if its content interests to the investigation, and, sometimes, extract some metadata. We show in this paper, that Microsoft Word can, under some circumstances, store older versions of a document. We also present a technique to extract these versions, where our program prove to be efficient to recover up to 12 older versions of a document.

***Index Terms*—Microsoft Word previous versions**

I. Introduction

The Microsoft Word is today one of the most utilized editors in the world. Due to this, the great majority of the medias seized in police procedures or in private investigations includes several files created with this program. Usually, the analysis of these documents is just verifying the relevance of the content to the case in subject and reporting it or not. Other information, called metadata, can also be extracted, such as author, company, title, date and hour of creation, modification, impression, etc.

However, we observed that, in some cases, the size in bytes of a Microsoft Word binary file increases, even if part of the text is deleted in several sessions of work. Opening the file with a hexadecimal editor, we verified that the deleted text still continues stored, in spite of not being more used by the editor.

The objective of this work was to study the binary structure of the files of Microsoft Word documents and to develop a tool to recover the texts already deleted, but still presents inside of the binary, what we called previous versions of the current document.

II. Structure of a Microsoft Word Document

We found published the binary formats of the documents of Microsoft Word 6.0 and of Microsoft Word 97 (version 8) in the site www.wotsit.org, however we did not find formats of more recent versions. The information presented in this work base on the binary format of the document of Microsoft Word 97 (version 8) [2], but tests and other references [3] show that the versions, until the Word 2003, possess similar structure. Microsoft announced that next version of Microsoft Word (Word 2007) will use XML as file format, altering the extension of .DOC to .DOCX, leaving the option to also utilize the format of the Word 97-2003 [3,4].

The information presented in this section are quite summarized and simplified to facilitate the understanding. More details are available in [2].

The documents created with Microsoft Word are binary files that follow the Microsoft OLE 2.0 (Object Linking and Embedding). This means that the Word uses the functions and procedures defined by standard OLE, which are available as a programming interface (API), to create and maintain a document. Thus, to access specific information inside a binary Word file, we should open it and to examine it through existent functions in the library of functions of API OLE.

The Word binary file is composed of several streams, and the ones that interest us are: main stream, summary information stream and table stream. The main stream consists of the Word file header (FIB - File Information Block), the text, and the formatting information. The FIB gives the beginning offset and lengths of the document's text stream and subsidiary data structures within the file. The summary information stream stores basic information, like the author name and company. The table stream containing several data structures that describes a document. In some cases, it is made a backup, and exists two streams, called 0Table and 1Table. The data structure that most interests us is the piece table, because it describes the logical sequence of the characters in a document. We called physical position of a character its position in the binary file and logical position its position in the document that the file represents, that is its position as visualized by the user in the moment of the edition with the Word.

III. Analysis of a Microsoft Word document

The analysis of documents produced with Microsoft Word or with other text editor is just, in most of the cases, verifying if its content links with the investigation in process. In some circumstances, it is also interesting to observe other information (metadata) embedded in the summary of the document, like, for example, author, company and date and hour of creation, modification and impression of the document. However, there are cases that the simple knowledge of the current content of the document and of the metadata attachment is not enough to form proofs. An example of that would be a case for which is important to know if the document suffered previous editions and which were the content of these previous versions. Let us imagine the situation where the analyzed document presents the content below:

" To Mr. John.
Please, make a deposit of US$ 100.000,00 in the account number 1234-5, Bahamas Bank, on the 10/10/2000.
Mr. Smith. "

Probably, a document of this type was sent by fax to Mr. John, whenever Mr. Smith needed of a deposit. Mr. Smith's normal procedure, whenever he needed a new deposit, it was open the document above and to alter the data that interest, as date, value, and account, and to send a fax to Mr. John with the new solicitation. As the document was altered and possibly safe, a new document won't be created. In a simple analysis, only the last deposit solicitation would be visualized. Probably, however, several solicitations based on this document may have happened before. Our work intends to present a solution for this demand of deeper Microsoft Word documents analysis.

IV. Proposed Solution

Motivated by the problem presented in the previous section, we studied the Word files based on empiric tests and in [2]. As our work involved a lot of Word non documented actions, they can vary from version to version.

The first verification during the work was that when the program option "Allow fast saves" is enabled and a certain document suffered several editions, the respective texts of previous editions will still exist in the binary of the file. That is easy to verify, just editing a document, and saving it some times. After that, if we open the document in a hex editor, the document may contain text that was previously deleted. Microsoft has already noted this behavior [6]. The forensic expert, however, doesn't know where those texts were located. It is important to stand out that the indexed search tools usually work on the text that those files represents, not indexing words that were deleted, but that can be inside of the binary of the file. Obviously a search in the whole content of the file would locate the deleted words.

The following step was to discover if, in some way, the piece table (table that describes the logical sequence of the characters in a document) registered these alterations. Even so, we verified that the piece table is static, storing only one version of the document. We also verified that Word uses two table streams, 0Table and 1Table, alternately to save the alterations in a complex document. This way, there would be at least two piece tables, one for the current document and another for the previous version, being possible, then, to recover the last version of the document.

In our tests, we observed that the physical location of the piece table inside of the file moves when it is created again, and the new one does not wipe the old table. With that, we started to seek for the previous piece tables and we verified that they continued intact inside of the file. That scenery is similar to what happens in FAT/NTFS file systems when a file is deleted: the file is marked as deleted, but its content and the reference to the file continue in the disk. The act of recovering the previous piece tables allows easily to extract the previous versions of the document since the piece table describes the logical sequence of the characters in a document and the characters in a complex document are not erased.

The structure of the piece table consists of two vectors of n positions, where n is the amount of disjoint blocks of text, stored sequentially. The first vector, called CP (Character Position), defines the partitioning of the document in non-continuous parts. The second vector, called PCD (Piece Descriptors), registers the physical position of each part of the text indexed by the CP vector. PCD also keeps the references for the formatting information of the text.

An indicator of one byte, represented by the number two, and the size in bytes of the piece table are stored before the vectors. An example of the vectors of the piece table is shown bellow, not considering the formatting information of PCD:

Index	1	2	3	4	5	6	7
CP Vector	0	5	16	24	30	50	60
PCD Vector	900	950	870	920	1000	1200	1100

This example shows that the document is divided in 7 text blocks. The first block, that stores the characters from 0 to 4, is located starting at the physical position 900. The second block, that stores the characters from 5 to 15, is located starting at the physical position 950, and so forth.

We developed an algorithm to locate possible piece tables inside of the table streams. The algorithm scans the whole

space of the table streams, seeking for a data structure similar to a piece table. Finding such structure, the text referenced is extracted as a previous version of the document. Step by step, we have the following:

1. Seek for the indicator 2;
2. Read 4 bytes, corresponding to the size in bytes of the piece table. This value should be smaller than the size of the file so that it is valid.
3. With the size, the amount of positions of the vector is calculated, that we called n, knowing that each position of CP occupies 4 bytes and each of PCD 8 bytes. The result for n should be integer so that it is valid.
4. Read n positions of 4 bytes and to verify if it is in ascending order.
5. Case all the previous steps succeed we considered that we found a piece table, and the text regarding it is extracted.

This algorithm was implemented in C and the corresponding program gets to recover with success texts of previous editions, since the document is complex and elaborated in the Word versions 97 to 2003. Microsoft says that occurs up to 15 fast save actions before a document is reconstructed [5], so it is, in thesis, possible to recover up to 15 versions. In tests, we got to recover up to 12 texts, being one of them the current version, because our program doesn't make distinction. It is not possible to determine a chronological order for the versions neither a pattern of behavior, because it is a not documented action of Word. In our tests it was not found any piece table by mistake, showing that the restrictions imposed above are enough to find the correct piece tables, without incurring in false positive. The largest limitation of the program is not recovery formatting information and objects (illustrations, graphs, videos, etc), that was left for a future work.

Besides the text, the program also extracts the list of the users' names that saved the document and the respective save directories. This function is documented in [2].

The tool is available for police institutions, by contacting the authors.

V. Conclusion

In this work we presented a technique that can be used by Forensic Computer experts to recover previous versions of Microsoft Word documents. These informations exist inside of the document binary file, even so in a way not documented and not accessible to the user. It is important to stand out that the indexation tools usually work on the updated text only, and they won't index words of previous versions.

We showed in which situations the Word store the previous versions, how the developed algorithm works, the results and the limitations of the developed tool. We left as future work the recovery of formatting information and objects (illustrations, graphs, videos, etc) of the document.

References

[1] *Microsoft Word 6.0 Binary File Format*, available at http://www.wotsit.org/download.asp?f=wword60.
[2] *Microsoft Word 97 Binary File Format*, available at http://www.wotsit.org/download.asp?f=word8.
[3] *Walkthrough: Word 2007 XML Format*, available at http://msdn2.microsoft.com/en-us/library/ms771890.aspx.
[4] *What's New for Developers in Word 2007*, available at http://msdn2.microsoft.com/en-us/library/ms406055.aspx.
[5] *Frequently Asked Questions About "Allow Fast Saves"*, available at http://support.microsoft.com/kb/291181.
[6] *Word Document That Is Opened in Text Editor Displays Deleted Text,* available at http://support.microsoft.com/kb/287081/EN-US.

Remoção de Proteções de Acesso a Dados Armazenados em Sistemas Computacionais – Ferramentas e Técnicas

Galileu Batista e Sérgio Xavier

***Abstract*— Media contents analysis is a recurrent aspect in computacional forensics. The most prominent techniques are full indexing and searchs relevant data. However, more and more data are managed by information systems, protected by passwords or other means. In this case, full access to the program offers an integrated view and can be essential for the investigation. This paper discuts several tools and techniques helpful to bypass information system's protection in forensics environment.**

***Index Terms*— Reverse Engineering, Software Tools, Programming.**

I. Introdução

A análise de conteúdo é um problema recorrente nas perícias em mídias computacionais. A indexação e posterior busca por cadeias de texto relevantes são procedimentos típicos nesses casos [1]. Há, porém, cada vez mais situações onde os dados estão organizados e são tratados por sistemas computacionais. Nessas situações é mais eficaz acessar os dados através do próprio sistema, que relaciona os dados e lhes confere significado mais apropriado. Na prática, o acesso a sistemas é, quase sempre, protegido, e, os mecanismos de acesso não disponíveis.

A liberação é um processo de cinco passos: 1) identificação da natureza do código executável do programa, especialmente no tocante ao compilador que o gerou; 2) Análise estática do programa, que permite a compreensão da sua estrutura global – decompiladores podem ser usados nesse passo, tornando o trabalho mais simples; 3) Análise dinâmica que permite envidenciar o fluxo de dados e controle do programa; 4) Localização: reduzir a análise aos pontos de implementação de proteções, e, 5) Modificação do programa para liberar as proteções.

Este artigo formaliza o contexto associado à liberação de proteções de programas binários x86 em ambiente Microsoft Windows®, as ferramentas e técnicas empregadas para esse propósito. A apresentação dessas técnicas na literatura é normalmente dispersa, considerando o potencial uso dessa informação. Trabalhos recentes discutem o tema: em [2] há um uma excelente introdução ao tema, incluindo seus aspectos legais; há também a descrição do uso de algumas técncias em situações hipotéticas, [3] discute conceitualmente o tema, sem apresentar uma metodologia de ação. A principal contribuição desse artigo é apresentar sistematicamente as técncias comumente usadas, mas não largamente documentadas. O texto está organizado como segue: a seção II discute a importância da identificação dos compiladores usados para gerar os programas binários para a seleção das ferramentas de liberação discutidas na seção III. Quando a reversão do código não é possível deve-se liberar as proteções diretamente no binário, empregando técnicas descritas na seção V. Antes da liberação, em si, é necessário identificar onde elas acontecem, o que pode ser conseguido com as técnicas da seção IV. A seção VI apresenta técnicas mais recentes de proteção, cuja liberação pode ser mais complicada. A conclusão está na seção VII.

II. Identificação do Programa Compilado

Arquivos compilados são o foco das liberações de proteções tratadas nesse artigo. Nesse sentido é importante identificar o compilador utilizado para converter o programa fonte em objeto, o que permite o uso de ferramentas específicas para guiar o processo de liberação. Por exemplo, um programa compilado usando *Borland Delphi*® pode ser mais facilmente compreendido se um decompilador *Delphi* for empregado.

A principal ferramenta de identificação de assinaturas de executáveis Windows é o *PEiD*[1]. A prática mostra que, em geral, os programas são resultantes de compiladores para as seguintes linguagens: *C*, *Delphi/C++ Builder*, *Visual Basic* e *Java*®, sendo o *PEiD* a ferramenta de identificação do compilador/ferramenta mais utilizada.

Com o surgimento de sofisticadas técnicas de engenharia reversa de código compilado e visando proteger propriedades intelectuais, desenvolvedores estão, cada vez, mais usando

G. Batista de Sousa é Perito Criminal Federal do Departamento de Polícia Federal, lotado no Setor Técnico Científico da Superintendência Regional em Pernambuco (e-mail: galileu.gbs@ dpf.gov.br). É também Professor do Departamento de Estatística e Informática da Universidade Católica de Pernambuco.

S. A. C. Xavier é Perito Criminal Federal do Departamento de Polícia Federal, lotado no Setor Técnico Científico da Superintendência Regional em Pernambuco (e-mail: sergio.sacx@ dpf.gov.br).

[1] Os autores optaram por não mencionar as URLs relativas a softwares, visto que as mesmas podem ser facilmente localizadas através de ferramentas de busca na Internet.

ferramentas que compactam e/ou cifram o código executável. Como resultado, essas ferramentas constroem um novo executável que contém código para reconstruir, em tempo de execução, o programa original. A técnica dificulta a liberação de proteções, uma vez que não é possível fazer atualizações diretamente no executável original, que se encontra compactado ou cifrado dentro de um novo programa.

Liberar programas ofuscados requer, como primeiro passo, evidenciar trechos de que implementam o processo de reconstrução, separando-os daqueles que formam o executável original em si. Esse procedimento pode ser bastante complexo, especialmente porque o processo de reconstrução pode se dar gradativamente e sob demanda [2].

O *PEiD* reconhece a assinatura da maioria dos ofuscadores e contém plug-ins que reconstroem o original em vários casos. Em outras situações é possível encontrar ou desenvolver ferramentas específicas, fazendo com que a maioria dos programas ofuscada possa ser reconstruída. Os programas encontrados no ambiente de perícias forenses (quando da escrita deste artigo) raramente contêm ofuscação.

III. Ferramentas de Análise do Código Executável

A análise do código executável pode ser feita apenas avaliando Há várias ferramentas para análise e execução do código executável genérico. As mais populares são os *debuggers* e/ou *disassemblers*: SoftIce®, IDA Pro®, WDAsm® e *OllyDbg*. A vantagem do *SoftIce* é a abrangência. O *WDAsm* tem a capacidade de abrir formatos mais antigos. *IDA Pro* e *OllyDbg* se equivalem, porém o segundo é gratuito, tem largo suporte da comunidade e um bom conjunto de *plug-ins*, razão pela qual será discutido nesse texto.

OllyDbg é um *disassembler* com *debugger* integrado que, além das funções típicas, realiza análise do código binário, identifica sub-rotinas e padrões de código gerados por compiladores para comandos estruturados, além de permitir a modificação do código binário durante a execução.

Programas escritos em *Delphi* ou *C++ Builder*® podem ser mais bem analisados usando o *Delphi Decompiler* (*DeDe*). O *DeDe* facilita a compreensão do código e permite a recuperação da aplicação, exceto as rotinas de manipulação de eventos, criadas pelo programador da aplicação, que permanecem em código de máquina. Além disso, o *DeDe* não permite mudanças diretas no código executável. O bom suporte à identificação de cadeias de caracteres e de nomes de funções e métodos da API do *Delphi* permite a localização de pontos de referência das eventuais proteções. Estas referências são fundamentais no processo de liberação, ainda que a liberação em si seja efetuada usando outra ferramenta, como o *OllyDbg*. Saliente-se a existência de um *plug-in* para o *OllyDbg*, denominado GODUP, que realiza funções similares ao *DeDe*.

A análise de programas em Java é simplificada em função do formato do *bytecode* e das características da máquina virtual. A natureza da linguagem, faz com que o *bytecode* possua as referências externas a outras classes expressas como cadeias de texto, permitindo-se identificar rapidamente a cadeia estática de chamada de métodos. Além disso, a JVM, por ser uma máquina de pilha, tem como característica um código de muito fácil leitura por humanos. Essas duas propriedades fazem com que existam decompiladores, por exemplo o *DJ Java Decompiler*, que retornam código fonte de alta legibilidade. Nesse sentido, a análise de proteções de programas escritos em Java pode, normalmente, ser feita no código fonte.

Programas escritos em *Visual Basic* (VB) também podem ser decompilados. Em verdade, o resultado, para as versões mais recentes do *VB*, é similar àquele obtido pelo *DeDe* para programas escritos em *Delphi*. Algumas ferramentas, como o *VBReFormer*, permitem a edição visual das propriedades dos formulários e objetos de gráficos presentes no arquivo executável, permitindo liberar proteções mais óbvias.

A Figura 1 apresenta um diagrama com os passos necessários à identificação do programa e as ferramentas adequadas para a liberação em cada caso. Na Tabela 1 estão sintetizadas características e aplicabilidade das ferramentas apresentadas.

Tabela 1 - Aplicabilidade de ferramentas de liberação.

Ferramenta	Aplicabilidade	Resultado da decompilação	Análise do código Binário
DJ Java Decompiler	Java	Código fonte em Java.	-
Delphi Decompiler (DeDe)	*Delphi* e C++ Builder	*Forms*, *resources* e *callbacks* (em *assembly*).	Reconhece referências a cadeias de *caracteres* e APIs *Delphi*.
VBReFormer	Visual Basic	*Forms*, *resources* e *callbacks* (em *assembly*).	Reconhece referências a cadeias de *caracteres* e APIs do *VB*.
OllyDbg	Qualquer executável (formato PE)	Código *assembly*.	Identifica sub-rotinas, variáveis, construções estruturadas e chamadas à APIs do Windows.

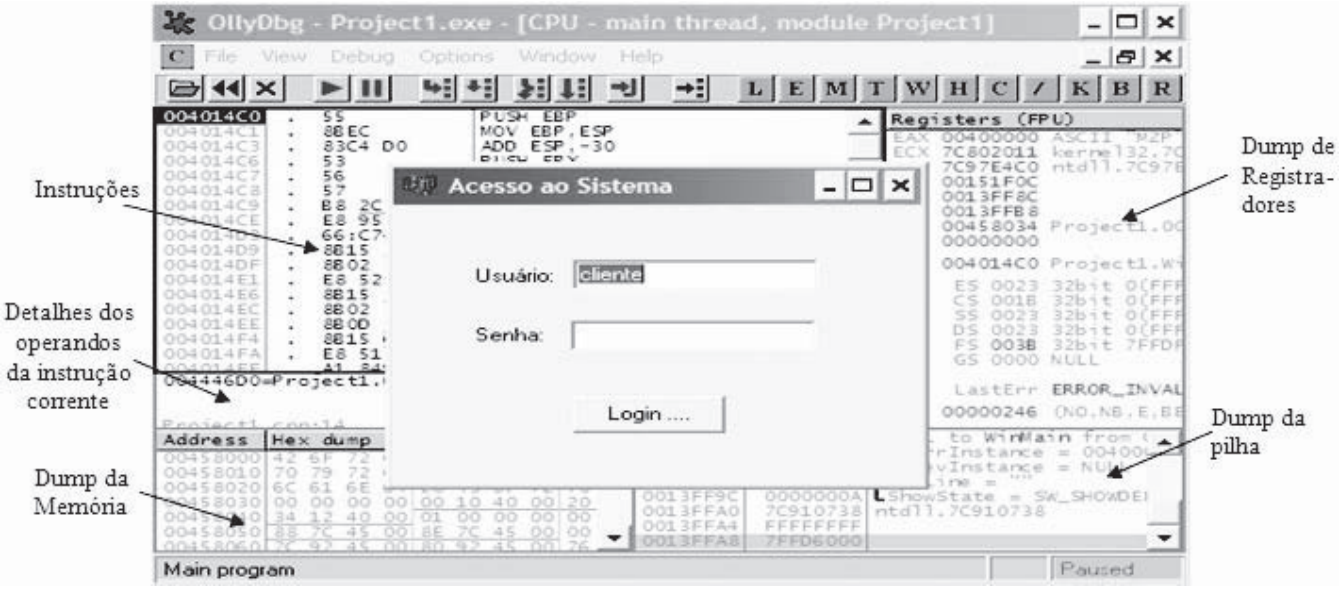


Figura 1 - Visão geral do OllyDbg, com uma aplicação sob *debug*.

IV. Identificação de Pontos de Validação

Considerando a existência de milhares, às vezes milhões, de instruções em um programa e suas bibliotecas associadas, encontrar o(s) ponto(s) que implementam as proteções, ou pontos de validação, é a parte mais complicada do processo de removê-la.

Há duas formas básicas de analisar código, objetivando descobrir pontos de validação: estática ou dinâmica. A análise estática (ou *dead-listing*) é feita seguindo manualmente o código, tentando prever o seu comportamento, sem executá-lo. A análise dinâmica usa um *debugger* para, executando o programa, entender o seu fluxo de dados e controle. Embora forneça uma melhor compreensão do programa, a análise estática é mais demorada e há casos, por exemplo, código ofuscado, onde ela é, praticamente, impossível.

As técnicas de análise dinâmicas variam desde a simples busca por usos de cadeias de caracteres no executável, até a identificação, na pilha de chamadas, de quais rotinas implementam proteções [3].

No contexto em análise, *DeDe* e *VBReFormer* são usados para identificação de *callbacks*. A partir disso e como nos demais casos, o trabalho de liberação é executado utilizando o *OllyDbg*, a única das ferramentas que tem capacidade de *debugging* e modificação do *assembly*, A Figura 1 apresenta a tela do *OllyDbg*, com um programa que lê uma senha e valida contra uma cadeia armazenada internamente, emitindo uma notificação de acerto ou erro. O programa foi escrito e em *C++ Builder* e será usado para as análises subsequentes.

A seguir serão discutidas várias técnicas empregadas para identificação de pontos de validação. Praticamente todos os casos compartilham um princípio: identificar um acontecimento e fazer uma análise da região do código próxima a ele, objetivando compreender o processo de validação. A proximidade diz respeito ao comportamento dinâmico do programa, ou seja, ainda que os trechos de código estejam em endereços muito diferentes, eles devem guardam alguma dependência em tempo de execução.

A. *Acessos a cadeias de caracteres e Chamadas a API*

A forma mais simples de identificar um ponto de validação é através do reconhecimento de instruções onde mensagens de erro ou alerta são emitidas. O *OllyDbg* tem a capacidade de buscar cadeias de caracteres e vincular as instruções que as a referenciam. Forçando paradas (*breakpoints*) em instruções próximas às mensagens pode-se evidenciar as razões que causaram o "erro" e entender a lógica por trás da validação.

Figura 2 - Visualização de instruções que acessam cadeias.

No *OllyDbg*, a visualização das instruções que acessam

cadeias de caracteres é feita através do menu de contexto da janela de instruções, seguido das seleções: (***"search for", "All referenced text strings"***). A Figura 2 mostra o resultado da busca por cadeias. Selecionando a linha **"Senha Incorreta!!!"** encontra o trecho de código mostrado na Figura 4, onde está o ponto de validação da proteção.

Por vezes, as cadeias de caracteres são propositalmente cifradas. Uma alternativa para encontrar pontos de validação é procurar por chamadas à API do Windows que realizam ações de criação de janelas (**CreateWindowEx**) e caixas de mensagens (**MessageBoxA**), exibição de textos (**DrawText**), uso de janelas de diálogo (**CreateDialogEx** e **EndDialog**), entre outras. Essas funções são tipicamente usadas para exibição de mensagens.

Usando a funcionalidade do *OllyDbg* de buscar instruções que referenciam chamadas a bibliotecas (acessível do menu de contexto da janela de instruções, seguindo as seleções: ***"search for", "All intermodular calls"***), é possível aplicar ações semelhantes aos casos onde as cadeias de caracteres não estão cifradas. A Figura 3 mostra a idenficação de **MessageBoxA**.

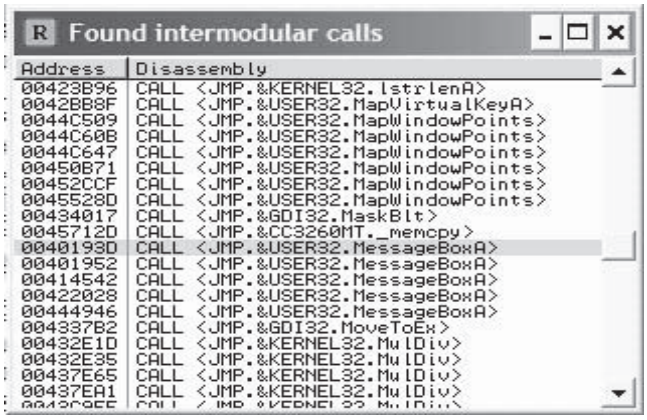


Figura 3 – Visualização de chamadas a bibliotecas.

Ressalte-se que a integração do *debugger* com o *Wingraph32* permite a visualização do fluxograma de uma sub-rotina, bem como dos diagramas de sub-rotinas que a chamam e que são por ela chamadas. Estas funcionalidades simplificam o trabalho de análise da proteção.

É bastante comum que as proteções sejam implementadas utilizando bibliotecas de terceiros. Nesses casos, a procura por cadeias de caracteres ou chamadas a API só deve ser realizada após a carga da biblioteca. Uma estratégia para descobrir o momento exato de realizar a busca é utilizar a funcionalidade ponto de parada após cada carga de biblioteca dinâmica.

B. *Parada em funções de tratamento de eventos*

Quando o acesso a cadeias e APIs é indireto, ou feito por bibliotecas que compõem o ambiente de tempo de execução da linguagem, não é possível usá-las como referências para identificação de pontos de validação. Uma alternativa é forçar paradas no início de todas as sub-rotinas de tratamento de eventos (*callbacks*). Ao executar o programa, pode-se remover as paradas que não se associam com a validação em si. Esse procedimento, típico para programas escritos em *Visual Basic*, permite identificar a rotina que implementa a proteção.

De uma forma geral, a viabilidade dessa técnica reside na capacidade de identificar inícios de sub-rotinas. Como a maioria dos ambientes de tempo de execução segue o que se denomina de "convenções de chamadas de sub-rotinas", o que no ambiente *Windows/x86* significa que as variáveis locais são acessíveis através do registrador "*base pointer*", EBP, é possível supor que uma sub-rotina inicia com **PUSH EPB**. A visualização dessas instruções é feita através do menu de contexto da janela de instruções, seguido das seleções: (***"search for", "All commands"***) e digitando ***PUSH EBP***.

Forçar paradas em todos as *callbacks* pode gerar efeitos ruins num primeiro momento, pois as rotinas de repintura e tratamento de mouse podem ser interceptadas. Contudo, gradativamente pode-se remover as paradas, restringindo-as à *callback* de validação desejada. Dentro da *callback* a análise pode prosseguir para frente, avaliando propriamente a validação.

C. *Memory Breakpoints*

Ocorre freqüentemente que uma notificação de erro foi emitida, tendo sido gerada muitas outras instruções atrás. Nessas situações pode ser difícil encontrar, observando apenas o ambiente próximo à exibição de uma mensagem, o ponto que efetivamente implementa uma validação. Associando paradas em acessos a posições de memória tem-se a oportunidade de identificação o momento de geração da mensagem na memória, tornando a análise mais efetiva e permitindo identificar mais facilmente os pontos de validação, não apenas de exibição de mensagens. No *OllyDbg*, pode-se ativar essa funcionalidade a partir dos menus de contexto das janelas de instrução ou de "*dump* de dados", seguindo: ***"breakpoint", "memory, on access"*** ou ***"memory, on write"***.

Essa técnica é fundamental quando o programa está, de alguma forma, cifrado, e nenhum decifrador está disponível. Com *breakpoints* de memória é possível identificar pontos de escrita no segmento de código, o que revela que o processo de decifragem está em curso. Com critério pode-se selecionar *breakpoints* na instrução que corresponde ao início original do programa (OEP). Descoberto o OEP é um passo importante para recompor o executável original, sem a rotina de decifragem. Pela forma de implementação de *breakpoints* convencionais não é possível usá-los para esse fim.

D. *Saída abrupta*

De alguma forma, as técnicas anteriores baseiam-se em informações oferecidas pelo mecanismo de proteção, como por exemplo: mensagens de erro e telas de registro. Um caso comum ocorre quando, após uma falha na validação da proteção, o programa termina sem quaisquer informações

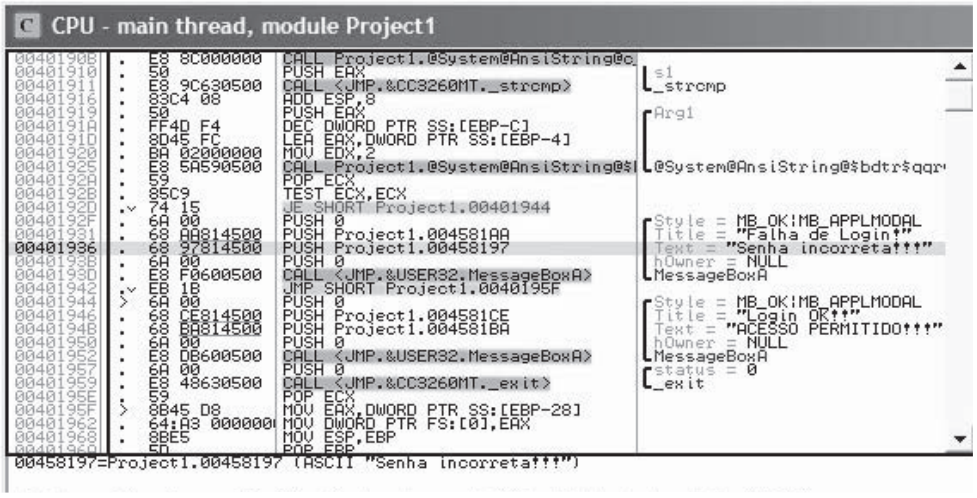


Figura 4 - Ponto de referência da validação da proteção.

adicionais. O tipo de análise adequado à situação é identificar chamada à rotina **`TerminateProcess`** (e suas variações) e acompanhar, via análise da pilha de chamadas, as condições que forçaram a sua execução.

É importante considerar que a chamada que termina o programa não necessariamente ocorre imediatamente depois da falha de validação. Proteções mais sofisticadas introduzem uma aleatoriedade no tempo entre os dois acontecimentos, dificultando a análise. Esse aparente *assincronismo* entre a validação e a notificação ou finalização do programa pode sempre ocorrer. Em geral a solução é identificar a propriedade que ao ser verificada, provoca o final do programa (ou mensagem de notificação), buscando, em seguida, as instruções em que ela é estabelecida. Quando a propriedade é um valor em uma posição de memória, deve-se fazer um monitoramento, usando *memory breakpoints,* dos trechos de código que a atualizam. A análise pode continuar, inclusive com o uso de outras técnicas, até que seja determinado o processo de validação como um todo.

A questão precedente reflete um fato: as técnicas de identificação não são completamente disjuntas, sendo aplicadas concomitantemente em várias situações. Normalmente, pode-se utilizar uma ou mais delas para reduzir o espaço de busca e, em seguida, aplicar outras.

E. Análise da Pilha de Chamadas

Quando as técnicas precedentes não são suficientes, uma técnica importante para reduzir o espaço de busca é a análise da pilha de chamadas. Observando o resultado visível de uma validação (tais como mensagens de erro, construídas dinamicamente) pode-se buscar a seqüência de chamadas de sub-rotinas que culminou com a ação. Avaliando as cadeias de caracteres presentes na pilha, pode-se estimar com precisão, qual das sub-rotinas a escreveu pela primeira vez, o que revela a proximidade do ponto de validação.

Em casos extremos, pode-se marcar pontos de parada em todas as chamadas de sub-rotinas presentes na pilha no momento da exibição da mensagem de proteção. Continuando a execução pode-se concluir que aquelas em que não houve parada não participam da validação. Por outro lado, a última chamada da seqüência em que houve uma parada, está, via de regra, muito próxima do ponto de validação.

O *OllyDbg* identifica pontos de retorno de sub-rotinas, bem como parâmetros de chamadas conhecidas (APIs) e endereços contendo cadeias de caracteres. Esses elementos podem ser visualizados na Figura 1, na janela de *dump* da pilha da Figura 1.

F. Análise para frente

Finalmente, há casos onde nenhuma informação efetiva sobre o ponto de validação pode ser conseguida empregando as técnicas precedentes. Uma análise do fluxo de controle do programa, partindo do seu ponto de entrada rumo às rotinas que implementam as funcionalidades, pode ajudar a compreender a estrutura geral do mesmo, e evidenciar ainda, que sem grande precisão, o ponto de validação.

Em certo sentido a análise para frente é sempre feita. Após identificar a vizinhança da validação, usando outras técnicas, é necessário compreendê-la efetivamente, o que é feito por análise para frente.

V. Remoção de Proteções

As técnicas de remoção da proteção podem ser classificadas em intrusivas e não intrusivas. No primeiro caso o executável é modificado para que a proteção seja removida. No segundo, um algoritmo de geração da senha, ou mesmo a própria senha, é descoberta, podendo ser usada para obter direta ou indiretamente o acesso irrestrito ao sistema.

As técnicas intrusivas mais simples consistem na inversão de uma instrução que verifica uma propriedade, por exemplo, a senha. Na Figura 4 a simples troca do mnemômico ***`JE SHORT Project1.00401944`*** por ***`JNE SHORT Project1.00401944`*** na instrução ***`40192D`*** resulta na liberação da senha de acesso ao programa.

Tabela 2 – Transformações que concretizam a liberação de proteções.

Código Original	Código final	Proteção
`JE END_OK`	`JNE END_OK`	Teste simples de condição que libera a execução completa do programa. Diversas outras condições ocorrem, sendo suficiente invertê-las.
`JNE END_OK`	`JE END_OK`	

`PUSH EBP`
`...`
Código da sub-rotina
`...`
`RETN`
	`MOV EAX, valor`
	`RETN`
		Modificação de sub-rotina de validação para sempre retornar um valor conveniente.

`CMP [MEM],valor` `JZ END_OK`	`MOV [MEM],valor` `JMP END_OK`	Modificação de um valor em memória que é usado em múltiplos pontos de validação. Esta mudança em um ponto, reflete-se em todos os outros.

O *OllyDbg* permite a alteração de instruções em tempo de execução, bastando selecionar (com barra de espaço) uma delas e reescrevê-la. Os devidos ajustes de tamanho também são realizados. Tendo modificação contornado a proteção, é possível construir um novo executável com essa propriedade. É um processo de dois passos:

- No menu de contexto da janela de instruções, deve-se selecionar: ***"Copy to executable", "All modifications"***).
- Como resultado da ação anterior uma nova janela de instruções é criada, na qual deve-se selecionar no menu de contexto a opção ***"Save file"***.

Outra técnica de proteção comum é a validação, em múltiplos pontos, de uma propriedade. Essa proteção é implementada, tipicamente, por testes do valor retorno de uma função de validação. A modificação do valor de retorno libera a proteção nos vários pontos. O mais simples nessa situação é substituir todo o corpo da função de validação por apenas duas instruções: 1***) MOV EAX, valor***; 2) ***RETN***. Aqui se supõe: ***EAX*** deve conter o valor de retorno da função; ***valor*** é um número consistente com a liberação (0 ou 1, normalmente).

Uma situação já discutida trata da validação que consigna seu resultado em uma posição de memória. Posteriormente, e em trechos arbitrários do programa, o valor dessa posição é verificado. A liberação pode ser feita em qualquer dos pontos que ocorrem as verificações. Ou seja, efetuando a substituição de um código da forma ***CMP [MEM],valor; JZ END_OK*** por ***MOV [MEM],valor; JMP END_OK***. Feita a substituição, as outras validações serão todas positivas.

Não são raras as situações onde a validação ocorre em uma *thread*, que é chamada periodicamente para validar ou estabelecer uma propriedade que será validada em outros pontos do programeiro caso é recorrente em programas que usam chaves de *hardware* (*dongles*). Em ambas as situações, uma vez determinados os pontos de validação, a combinação das três técnicas acima é, em geral, suficiente para liberar a proteção.

A Tabela 2 apresenta um resumo das transformações necessárias para liberação do código em cada situação.

VI. TÉCNICAS ANTILIBERAÇÃO

A facilidade de remoção de liberações decorrente do avanço das ferramentas provoca contrapartidas também nas técnicas de proteção. Mesmo quando o código não está ofuscado, há um conjunto de técnicas correntemente em uso para dificultar a liberação das proteções:

- Identificação de presença de *debugger*: a tabela de ambiente de processos (PEB) do Windows armazena informações para caracterizar se um processo está ou não em depuração. A chamada à API **`IsDebuggerPresent`** ou o acesso direto à PEB fornece a informação. Para conveniência, o *OllyDbg* oferece um *plug-in* que "sobrepõe" a API e impede que a condição seja verdadeira.
- Cálculo de verificadores de integridade: é comum fazer verificações se o código do processo foi modificado. Uma função é aplicada sobre valores de posições de memória e testado contra um valor esperado. Em caso de falha o processo é terminado. Quando o resultado da integridade é usado como chave para decifrar um valor, que corresponde a um endereço de um trecho de código a ser executado, pode ser complicado remover a proteção.
- Acesso indireto a bibliotecas do sistema: ocorre quando as chamadas às funções da API estão codificadas por endereço, não por nomes. Essas chamadas implícitas tornam muito mais difícil buscar por pontos com funcionalidades conhecidas.
- Divisão de funções em blocos: é a técnica de subdividir uma função em blocos, colocados em endereços distantes uns dos outros. A execução de cada bloco é ativada por desvios, implementados como chamadas/retornos de função. O código, mais ineficiente, perde em coesão e significado,

ficando pouco aparente a sua real semântica.

- Cifragem e decifragem dinâmicas: quando uma função é crítica em significado, uma proteção eficaz é mantê-la cifrada no programa executável. Para a execução, ela é decifrada, executada e novamente cifrada. Como não permanece na memória, não é possível, estaticamente, definir pontos de parada sobre ela, nem tampouco é eficaz modificá-la. Nesses casos, somente uma análise para frente demorada, com eventual substituição de código pode liberar a proteção.
- Metamorfose de código: a técnica mais sofisticada de antiliberação envolve manter no programa executável um conjunto de rotinas que "reescreve" trechos críticos a cada execução. Entre as mudanças podem estar: renomeamento de registradores, seleção de instruções distintas e divisão de funções em blocos [4, 5, 6].

Algumas das técnicas acima descritas fazem com que o processo de liberação seja difícil o suficiente a ponto de torná-lo inviável. Pode-se dizer, contudo, que no ambiente forense, as técnicas de liberação continuam válidas, pois a maioria dos programas encontrados não tem como foco a proteção em si, mas o seu domínio de aplicação.

VII. Conclusões

Este artigo introduz um conjunto de técnicas e ferramentas usadas para a liberação de proteções. Por se tratar de um tema polêmico, há várias restrições na sua divulgação oficial, tornando difícil a efetiva compreensão do tema. Esse artigo visa contribuir para reduzir essa lacuna e implica, por outro lado, que as técnicas refletem a experiência dos autores na liberação de proteções em vários casos, porém não é possível garantir que sejam as únicas ou mais efetivas.

Finalmente, os autores reconhecem a sensibilidade do assunto analisado e não se responsabilizam, nem apóiam, qualquer uso, implícito ou explícito, das técnicas aqui discutidas, para finalidades ilícitas. Ressaltam também que o texto reflete suas opiniões pessoais, não das instituições a que estão vinculados.

Referências

[1] Galileu Batista, "A Perícia em Mídias de Armazenamento Computacional." Notas de Aula, Academia Nacional de Polícia. 2006.

[2] E. Eilam, "REVERSING: Secrets of Reverse Engineering." Indianapolis: Wiley Pusblishing, Inc. 2005.

[3] G. Hoglund, G. McGraw, "Como quebrar códigos – A arte de explorar (e proteger) software." São Paulo: Pearson Makron Books, 2005.

[4] K. Cooper, L. Torczon, "Engineering a Compiler." New York: Morgan Kauffman, 2003.

[5] M. Jürgen, "Metamorphic Code", disponível online em www.iaik.tugraz.at/teaching/03_advance%20computer%20networks/ss2006/vol12/Metamorphic-code-prenner.pdf

[6] _, "Enhancing software protection with poly-metamorphic code". New South Wales Society for Computers and the Law Journal (6), June 2004.

Detecção de Adulterações em Imagens Digitais

Sérgio Xavier, Galileu Batista e Eduardo Amaral

***Abstract* — Today's image manipulation software makes tampering digital photographs accessible to the common user. Digital hoaxes arise all over the Internet. Some of these forgeries have criminal implications. This paper discusses several techniques to identify signs of these forgeries so the investigator can verify whether a digital image is authentic or not.**

***Index Terms*— Digital Forgery, Tampering, Digital Image.**

I. Introdução

Gostemos ou não, imagens adulteradas – as conhecidas montagens – estão em todos os lugares e fazem parte de nossa cultura hoje em dia. Graças à popularidade das câmeras digitais e a disponibilidade de softwares de edição de imagens, essas falsificações se tornaram "lugar comum", especialmente na Internet.

Nós vemos muitas imagens que desafiam o senso comum e é natural questionar sua autenticidade. A maioria de nós já viu imagens que são obviamente falsas, como uma imagem de um gato gigante escalando o cristo redentor, mas naturalmente assumimos que não passam de montagens criadas simplesmente para nosso divertimento. Entretanto, há vários casos em que uma montagem é divulgada como sendo real, deixando a nosso critério decidir se determinada imagem é real ou não.

Várias dessas montagens possuem fins ilícitos – de meras difamações até crimes eleitorais – cabendo à Perícia Criminal analisá-las e determinar se são autênticas ou se não passam de falsificações.

A perícia de imagens – sejam elas digitais ou não – deve-se basear mais do que no simples bom senso do perito. Ela deve ser fundamentada em uma metodologia de análise que, baseada nas evidências encontradas, permita determinar a sua autenticidade.

Infelizmente não há um método infalível para determinar se uma imagem é autentica. Entretanto, se entendermos como as adulterações são feitas e soubermos quais características da imagem analisar, poderemos detectar a maior parte dessas adulterações.

O presente trabalho visa descrever técnicas que permitam ao Perito encontrar evidências de adulterações em imagens digitais, a fim de determinar a sua autenticidade.

II. Um pouco de história

Adulteração de imagens não é algo novo e nem recente. Alguns dos mais conhecidos exemplos de adulterações de filmes fotográficos, por exemplo, datam dos primeiros anos da extinta União Soviética, onde tanto Lênin como Stalin costumavam remover os "inimigos do povo" dos registros históricos. (**Figura 1**). Essas e outras adulterações similares eram criadas utilizando manipulações de imagens tais como: clareamento, escurecimento, retoque, spray e ajuste de cores e contraste. [5]

- A técnica do spray funciona através do uso de uma pistola (em formato de lápis) que borrifa tinta líquida, em baixa pressão, com o auxílio de ar comprimido.
- Os retoques são realizados diretamente sobre a película do filme com um pincel de ponta bem fina.
- Clareamento e escurecimento são manipulações que mudam a intensidade da exposição, sendo utilizadas máscaras fotográficas para delimitar as áreas afetadas.
- O controle de cores e contraste é realizado com o auxílio de filtros de luz especiais e papel fotográfico.

Figura 1: Acima, a foto original de Stalin e Nikolai Yezhov. Abaixo, a versão alterada onde Yezhov foi removido.

Todas estas manipulações requerem um alto grau de conhecimento técnico e material fotográfico sofisticado, que, em geral, estão fora do alcance da maioria das pessoas.

Nos últimos anos, câmeras digitais de alta resolução, a preços acessíveis, vêm rapidamente substituindo suas contrapartes baseadas em filme fotográfico. Além disso, o advento de computadores de baixo custo e alto desempenho e sofisticados softwares de manipulação de imagens e computação gráfica permitiram ao usuário mediano realizar

manipulações complexas em imagens e criar montagens com relativa facilidade.

III. Imagens Digitais

Uma imagem digital é, essencialmente, uma matriz de números, onde cada número representa o tom de cada ponto que compõe a imagem, também chamado de *pixel* (**Figura 2**). Uma imagem de 8-bits pode ter 256 tons de cinza. Uma imagem colorida é feita através da combinação de três imagens, cada uma representando uma das cores básicas: vermelho, verde e azul (RGB). A adição de diferentes quantidades dessas três cores básicas produz todas as demais cores do espectro. [1]

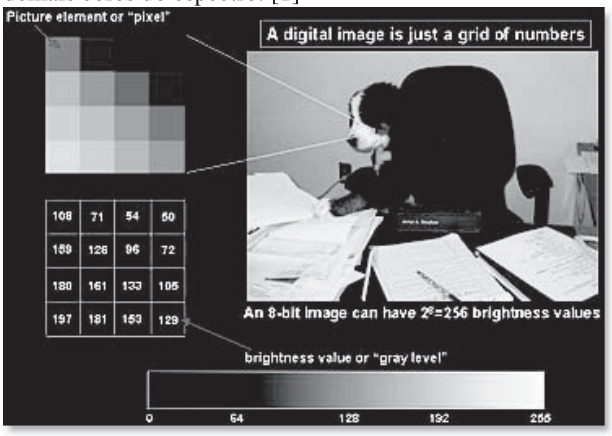


Figura 2: Uma imagem digital é simplesmente um array de números correspondentes aos tons da imagem.

Uma câmera digital funciona tal qual uma câmera tradicional, mas não requer filme para armazenar as imagens. Em vez disso, as imagens são armazenadas em chips de memória no interior da câmera. As imagens são capturadas por um dispositivo chamado *charged-coupled device* (CCD): uma coleção de milhares de células foto-sensíveis. Quando essas células são atingidas por um raio de luz, elas emitem sinais elétricos, que depois são convertidos na imagem digital.

IV. Adulterações em Imagens Digitais

Sendo, uma imagem digital, apenas um conjunto de números, é tecnicamente possível a um artista criar uma imagem "artificial" simplesmente escolhendo cada um dos números adequadamente para representar qualquer objeto ou cena que poderia ser capturado por uma câmera digital. Para uma imagem colorida (24 bits por *pixel*), há mais de 6 milhões de valores possíveis para cada *pixel*. Uma imagem 10cm x 15cm a 300 ppp (pontos por polegada) terá mais de 2 milhões de *pixels*, dando um total de mais de 36.000.000.000.000 de alternativas a considerar para se gerar uma imagem colorida.

Na verdade, nem todos os números possíveis precisam ser considerados pelo usuário, mas importantes considerações precisam ser feitas para se escolher os valores de cada *pixel*, principalmente quando iluminação e bordas são consideradas. Se uma imagem gerada por computador deve parecer ser real, então a imagem deve ser consistente com todas as leis da física aplicáveis às imagens reais.

Para se criar uma imagem digital que pareça real, os valores corretos de brilho devem ser escolhidos *pixel* a *pixel*, o que poderia levar meses (ou mesmo anos), dependendo do tamanho da imagem, sem a ajuda de software de computador para efetuar os cálculos. Esse tempo diminuiu bastante após o advento de softwares de computação gráfica, projetados para gerar imagens de objetos 3D com condições de iluminação realistas. Uma operação de renderização adiciona iluminação, sombras cores e texturas a um modelo de objeto que é criado pelo artista.

Modelos baseados na técnica de *Ray-Tracing* produzem os melhores resultados pela projeção de vários raios de luz e pela modelagem das interações desses raios com os objetos da cena, incluindo reflexão, refração e outros. O usuário deve simular uma quantidade suficiente de raios para cobrir todos os pontos da imagem, o que pode ser um processamento muito demorado. Os resultados são impressionantes e podem ser vistos em filmes de cinema. Entretanto, essa técnica é pouco utilizada na produção de imagens falsas devido à quantidade de cálculos necessários, sua complexidade e pelo fato do software envolvido não estar, geralmente, acessível ao usuário comum. (**Figura 3**)

Figura 3: Imagens geradas por computação gráfica com o auxílio dos softwares Maya, Mental Ray e Photoshop.

A maneira mais comum de se falsificar uma imagem, devido a sua simplicidade, é alterar uma imagem já

existente, que tenha sido capturada por uma câmera. A imagem pode ser alterada de duas formas: pela mudança de contexto e pela mudança de conteúdo.

A. *Mudança de Contexto*

Uma imagem pode ser alterada pela mudança de seu contexto. Um exemplo seria afirmar que uma imagem de uma lâmpada acesa é, na verdade, uma nave espacial alienígena.

Criar uma imagem falsa pela mudança de contexto tem sido, historicamente, o método preferido para se criar boatos, porque não necessita de nenhuma alteração na imagem, sendo a mesma uma imagem real. Dessa forma, a imagem (e seu negativo, se existir), vai passar por todos os testes científicos de verificação de autenticidade. Um exemplo conhecido é a famosa foto do monstro do Lago Ness, tirada em 1934 e que só foi confirmada como sendo falsa, após a confissão do autor, muitos anos depois. (**Figura 4**)

Figura 4: Foto do monstro do Lago Ness. Na verdade não passa de um submarino de brinquedo com uma cabeça de serpente anexada.

B. *Mudança de Conteúdo*

Tornou-se muito utilizada com o advento de softwares de tratamento de imagem de baixo custo, permitindo a qualquer um alterar rapidamente as imagens de forma criativa. As principais técnicas utilizadas nesse tipo de adulteração são:

- Composição: Uma das formas mais comuns de adulteração em imagens digitais, onde duas ou mais imagens são coladas juntas para a criação da montagem. A abordagem mais utilizada é simplesmente retirar uma parte de uma imagem e colá-la (digitalmente) em outra. O software permite ao usuário modificar a imagem recortada de forma a ajustar tamanho, rotação, brilho, etc. (**Figura 5**)

Figura 5: Montagem realizada por composição. O tubarão está iluminado a partir da frente enquanto que o resto da imagem está iluminado por trás.

- Retoques: É uma ampla classe de técnicas de adulterações que incluem spray, clareamento, escurecimento, desfocagem, cópia e colagem de regiões dentro da imagem. Softwares como o *Adobe Photoshop*™ e o *The Gimp* possuem uma grande variedade de ferramentas para retocar imagens. A **Figura 6** ilustra vários desses recursos.

Figura 6: Imagem original (acima) e imagem retocada (abaixo). Parte da barba foi removida e os dentes foram clareados.

V. Identificando Adulterações

Se uma imagem é suspeita, deve-se, primeiro, procurar pistas por inspeção visual e, se necessário, prosseguir com uma inspeção científica.

A primeira técnica a se considerar na identificação de adulterações é a própria percepção do Perito. A habilidade de sentir que há algo errado com a imagem, seguindo o bom senso, funciona na maioria das vezes. Se uma imagem parece ser inacreditável, então ela provavelmente não é verdadeira. Na **Figura 7**, o gato é obviamente grande demais para esta raça específica e o homem deveria estar mais curvado para segurar um animal tão pesado adequadamente.

Figura 7: O tamanho exagerado do gato sugere que há algo errado com a imagem.

Conhecimento sobre a tecnologia disponível na época em que a fotografia foi supostamente tirada pode, também, ajudar a determinar a veracidade de uma imagem. A montagem mostrada na **Figura 8**, dificilmente seria conseguida com o equipamento antigo (e pesado) disponível na época, principalmente dentro de um avião da primeira guerra mundial em pleno combate aéreo.

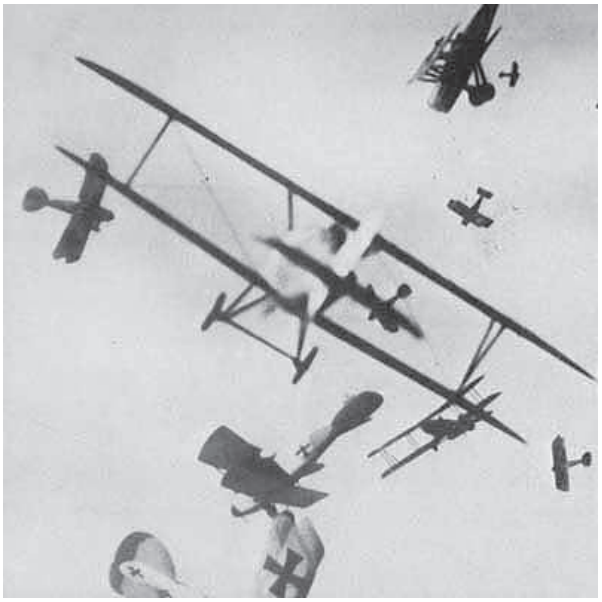


Figura 8: Cena de combate aéreo da primeira guerra mundial.

Uma adulteração realizada pela mudança de contexto é a mais difícil de detectar, pois na verdade a imagem é verdadeira, apenas o motivo da imagem é falso. A chave para se identificar uma imagem adulterada por mudança de contexto é identificar aspectos das imagens que são inconsistentes com sua descrição. Por exemplo, a data e hora do dia em que a imagem foi supostamente tirada podem ser inconsistentes com a posição do sol ou condições climáticas para aquela data.

Quando uma imagem é adulterada pela mudança de conteúdo, deve-se esperar que a parte alterada tenha inconsistências físicas que possam ser detectadas. Infelizmente, essas inconsistências nem sempre são aparentes e uma adulteração pode não ser descoberta até que a imagem original seja encontrada. A **Figura 9** ilustra uma alteração onde o rosto de uma atriz foi invertido, rotacionado e transferido para o corpo de uma outra modelo.

Figura 9: Montagem realizada por mudança de conteúdo. No detalhe, a inclinação do brinco denuncia a adulteração.

O processo de formação da imagem na câmera deve ser consistente com as leis da física de uma forma coerente em todos os pontos da imagem. Quaisquer incoerências podem ser indícios de adulteração. Os pontos a analisar são: condições de iluminação, resolução, mudança de tons, escala, gravidade, perspectiva e ruído.

Uma inconsistência comumente encontrada é a falha nas condições de iluminação. A parte alterada pode apresentar sombreamento inconsistente, indicando que foi iluminado em condições diferentes do resto da imagem (**Figura 5**). Além disso, deve-se considerar a iluminação difusa que ilumina o resto da cena. Diferenças aparecem quando um objeto fotografado com o auxílio de flash é adicionado a uma imagem com iluminação natural ou de estúdio.

Deve-se tomar cuidado ao analisar as características de iluminação de uma cena. As condições de iluminação e sombra podem levar ao erro, especialmente se aspectos referentes às três dimensões não forem considerados. A **Figura 10**, mostrando o pouso da Apollo 11 na lua, apresenta anomalias na direção das sombras, que podem ser explicadas pela topografia do terreno.

Figura 10: Imagem dos astronautas da Apollo 11 na lua. As sombras apontam para direções diferentes.

Normalmente, quem produz uma imagem adulterada ignora os recursos normalmente encontrados nas imagens reais, produzidas por uma câmera. Os efeitos mais significativos são: o realce das bordas, influenciado pela difração da lente, o foco, o desfocado causado por movimento (*motion blur*), a perspectiva e o ruído.

Quando um objeto é adicionado ou removido de uma imagem, uma borda com nível de realce inconsistente com o resto da imagem é, geralmente, criada. Esse realce é facilmente visível, de forma que é um sinal óbvio de que a imagem foi alterada, de forma que, ferramentas de desfocagem em softwares de manipulação de imagens são utilizadas para reduzir a visibilidade dessas bordas. Essa desfocagem, entretanto, vai produzir bordas borradas ao redor do objeto que serão inconsistentes com o resto da imagem.

Todos os objetos em uma imagem devem, também, estar na mesma perspectiva. Se a geometria de um objeto da imagem é inconsistente com a dos demais objetos, então ele, provavelmente, foi adicionado a partir de outra imagem. Por exemplo, em uma imagem autêntica, linhas paralelas convergem para o mesmo ponto, conhecido como ponto de fuga. Se linhas paralelas de um objeto não convergem para o mesmo ponto de fuga, então este objeto não pode ter sido fotografado pela mesma câmera que o resto da imagem. (**Figura 11**)

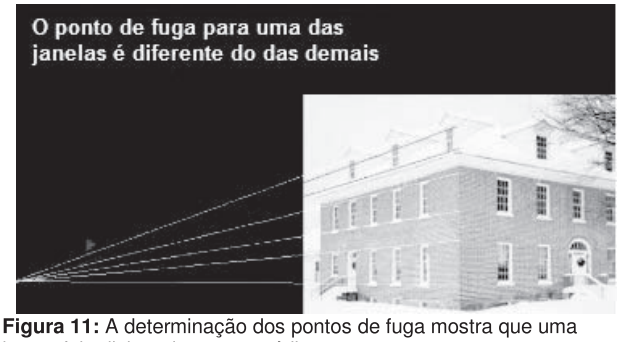


Figura 11: A determinação dos pontos de fuga mostra que uma janela foi adicionada a este prédio.

Para dar um efeito mais realista à adulteração, principalmente quando o objetivo é remover um objeto da imagem, é comum utilizar regiões da própria imagem para substituir os objetos que se quer ocultar. Em uma imagem autêntica, embora haja áreas muito parecidas, dificilmente será encontrado duas regiões exatamente iguais. A **Figura 12** ilustra esta técnica.

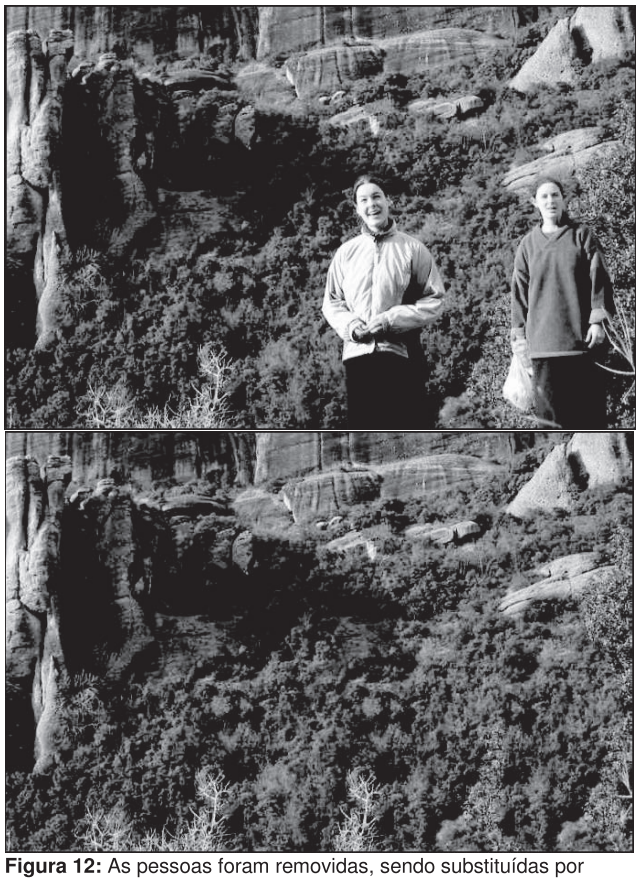


Figura 12: As pessoas foram removidas, sendo substituídas por outras regiões da própria imagem.

Infelizmente, a tarefa de dividir a imagem analisada em micro-regiões e comparar uma a uma é muito custosa para se realizar manualmente. Software especializado é necessário para viabilizar esta tarefa.

VI. Avanços Recentes

Pesquisas recentes estão desenvolvendo softwares que permitirão análises detalhadas das imagens que são impraticáveis de se realizar atualmente, mesmo com o auxílio de softwares de edição de imagens. Dentre os trabalhos de maior importância, podemos destacar:

- Farid e Popescu [4] e [5], do *Dartmouth College*, desenvolveram uma série de ferramentas, baseadas em técnicas estatísticas, capazes de detectar inserção de objetos nas imagens, alteração de cores, compressão JPEG dupla, regiões duplicadas e padrões de ruídos inconsistentes.
- Fridrich et al [8] e [9], da *State University of New York*, desenvolveram uma ferramenta que verifica se uma imagem digital foi fotografada em uma determinada câmera. Seu software baseia-se no fato de que cada câmera digital introduz um padrão de imperfeições único nas imagens capturadas. Esse padrão determina uma espécie de assinatura da câmera, que pode ser comparada com as características da imagem.

O trabalho de Farid e Popescu foi desenvolvido utilizando o software Matlab. Uma versão em Java está sendo desenvolvida neste momento e, em breve, estará disponível gratuitamente para os órgãos policiais de todo o mundo.

VII. Estudo de Caso

Em Setembro de 2006 foi enviado ao SETEC/SR/DPF/PE uma solicitação de perícia referente a uma investigação sobre falsificação de documentos com possível participação de funcionários do serviço de identificação da Secretaria de Defesa Social do Estado de Pernambuco. O material questionado consistia, dentre outros, de um arquivo em formato Microsoft Word (doc) contendo imagens de cédulas de identidade em branco. Um dos quesitos buscava determinar se as imagens haviam sido digitalizadas a partir de uma cédula de identidade já preenchida ou de uma cédula de identidade em branco. A **Figura 13** ilustra algumas das imagens encaminhadas a exame.

A análise detalhada das imagens em software especializado de manipulação de imagens (*Adobe Photoshop*™ e *IrfanView*) revelou uma série de detalhes das imagens:

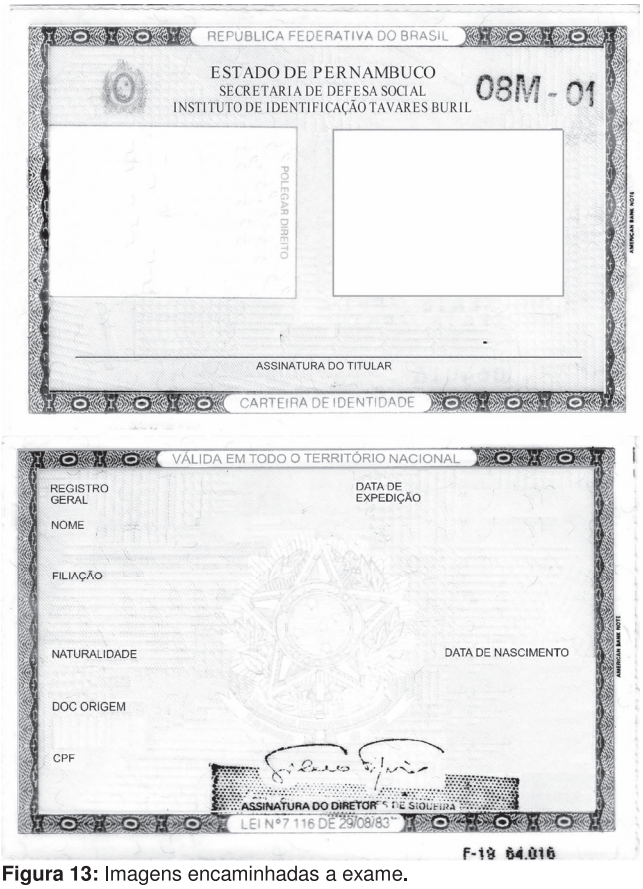


Figura 13: Imagens encaminhadas a exame.

- O padrão de fundo da imagem é consistente com o modelo de identidade utilizado pela Secretaria de Defesa Social de Pernambuco.
- Trechos contendo fibras de segurança repetidas, indicando que áreas da cédula onde estariam os dados do cidadão haviam sido sobrepostas. (**Figura 14**)

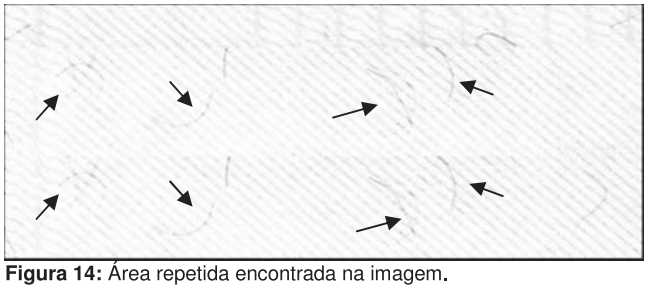


Figura 14: Área repetida encontrada na imagem.

- Textos com resolução maior que o resto da imagem, indicando que foi adicionado posteriormente. (**Figura 15**)

Figura 15: O texto à esquerda foi refeito após digitalização da imagem, por isso apresenta melhor definição que o texto à direita.

- Texto mal posicionado e erro de grafia no símbolo das armas nacionais. (**Figura 16**)

Figura 16: Texto contido no símbolo das armas nacionais foi reescrito ligeiramente fora da posição original e com um erro de grafia.

A partir desses indícios (e de outros que não foram incluídos neste trabalho), os Peritos concluíram tratar-se de uma imagem digitalizada a partir de uma cédula de identidade já preenchida.

VIII. Conclusões

Esse artigo apresenta uma série de técnicas utilizadas para a identificação de adulterações em imagens digitais. A maior parte dessas técnicas pode ser utilizada com o auxílio de software de baixo custo, facilmente acessível.

Embora as técnicas aqui descritas possam ajudar na detecção de muitas das adulterações, não há, atualmente, uma maneira de impedir que alguém, dispondo de tempo e recursos suficientes, crie uma montagem que não seja possível identificar. O que devemos esperar é que inconsistências possam ser encontradas, indicando que a imagem analisada é, de fato, uma montagem.

IX. Referências

[1] R. Fiete, “Photo Fakery”, http://oemagazine.com/fromTheMagazine/jan05/pdf/photofakery.pdf

[2] D. Brugioni, “Photo Fakery: The history and techiques of photografic deception and manipulation”, Brassey’s Inc, 1999.

[3] H. Farid. “Creating and detecting doctored and virtual images: Implications to the child pornography prevention act.”, Technical Report TR2004-518, Dartmouth College.

[4] A. Popescu e H. Farid, “Exposing digital forgeries by detecting duplicated image regions”, Technical Report TR2004-515, Dartmouth College.

[5] A. Popescu, “Statistical tools for digital image forensics”, Technical Report TR2004-531, Dartmouth College.

[6] The Museum of Hoaxes, www.museumofhoaxes.com.

[7] J. Fridrich, D. Soukal e J. Lukas, “Detection of Copy-Move Forgery in Digital Images”, Proc. of DFRWS, 2003.

[8] J. Fridrich, J. Lukas e M. Goljan, “Determining Digital Image Origin Using Sensor Imperfections”, Proc. SPIE Eletronic Imaging, 2005.

[9] J. Fridrich, J. Lukas e M. Goljan, “Digital Câmera Identification from Sensor Pattern Noise”, IEEE Transactions of Information Security and Forensics, vol. 1(2), pp. 205-214, Junho de 2006.

A NOTA FISCAL ELETRÔNICA E O ATUAL CENÁRIO DO CIBERCRIME. TEMA PARA O TRABALHO PREVENTIVO DO INSTITUTO NACIONAL DE CRIMINALÍSTICA DA POLÍCIA FEDERAL

*Coriolano Aurélio de Almeida Camargo Santos, Almeida Camargo Advogados.

Resumo* - O presente estudo, ao abordar o Projeto "Nota Fiscal Eletrônica", suscita as fragilidades deste instrumento de controle fiscal, na eventualidade de crimes eletrônicos. Aborda os pontos sensíveis do projeto[i] , pretendendo com isso remeter o leitor a uma reflexão sistêmica da convivência da NF-E em meio a códigos brutalmente sofisticados e maliciosos[ii], que podem acarretar graves problemas legais, muitas vezes camuflados em meio ao arsenal de produtos e materiais ilegais oferecidos na Internet. Reprova-se a idéia do surgimento da Nota Fiscal Eletrônica como panacéia fiscal do Século XXI e frisa-se que o ataque de *botnets* em larga escala, tornará frágil o sistema de alimentação da base de dados do fisco e de contribuintes. Aspira-se responder que o desenvolvimento tecnológico sustentável requer investimento contínuo em segurança, que a eficácia de qualquer projeto de controle fiscal eletrônico representa grande avanço, contudo um dos grandes desafios será a criação de mecanismos ainda mais inteligentes para impedir a ação de fraudes. Uma posição conservadora busca a realidade em acontecimentos atuais. Novos conceitos tratam de ponderar sobre a capacidade da Administração Fazendária para superar e prever a sagacidade e disfarce de facções e organizações[iii] criminosas, cada vez mais perigosas[iv] e altamente especializadas no seqüestro, furto, adulteração, danificação, controle ou geração da perda proposital de informações confidenciais do fisco, acarretando na quebra do sigilo fiscal do contribuinte.[v]

Palavras-Chave - Nota Fiscal Eletrônica, Cibercrime, Adulteração e Perda de Informações Fiscais, Análise de Risco, Atual Cenário.

I- Introdução

O presente artigo vem tratar dos riscos envolvendo o cibercrime. Os momentos de meditação aqui propostos são decorrentes da experiência do autor no exercício da advocacia, na análise de cibercrimes, no estudo de pesquisas de campo para elaboração de palestras, bem como, pela participação em trabalho colaborativo proposto no ano de 2.005 à Diretoria da Polícia Federal, que culminou em um trabalho de excelência a toda a sociedade. Em prol do aprimoramento da segurança do projeto da Nota Fiscal Eletrônica, sugiro que a Administração dos Negócios Fazendários dos Estados venham a utilizar como espinha dorsal, uma aliança Fazendária com o Instituto Nacional de Criminalística da Polícia Federal - INC. Dentro deste contexto, a Fundação Instituto de Administração (FIA), da USP[vi], recomendou a Secretaria da Fazenda de São Paulo uma maior interligação com outros órgãos cujas informações ou processos estejam inter-relacionados com os da Fazenda. Por fim, cabe registrar no corpo do texto, recomendação da assinatura de um importante Convênio de cooperação entre as Secretarias de Fazenda e o órgão de criminalística da Polícia Federal. Desta forma, poderia ser realizado um redesenho do Projeto da Nota Fiscal Eletrônica com foco em integrar ações voltadas a métodos preventivos contra a fraude eletrônica.

II - A Nota Fiscal Eletrônica e a Evolução do Cibercrime no Brasil.

Independente do grau de evolução das tecnologias de segurança, o combate às pragas digitais é "uma guerra infinita" e algumas empresas privadas ainda não têm este conceito. Deixar de lado a segurança é condenar a sociedade moderna. Sentir o perigo e permanecer inerte é proporcionar ao cibercriminoso o caminho e o meio que tanto deploramos. Discutir com os que acreditam que a Nota Fiscal Eletrônica é mecanismo absolutamente seguro e inviolável é prejudicar a exposição da verdade. Os que defendem esta posição "leva-nos a dizer coisas que não queremos, a formular paradoxos, a exagerar nosso pensamento e a deixar de lado a parte essencial de nossa doutrina para contrapor **truques de lógica,** aos escorregões que nos provocam[vii]". Contudo, a solução para o tráfego e guarda de documento público eletrônico é veiculado como permanente e absolutamente robusto. Trata-se de clara propaganda enganosa. O Projeto NF-e tem como objetivo a implantação de um modelo nacional de documento fiscal eletrônico. Pretende substituir a sistemática atual de emissão do documento fiscal, o qual equivocadamente, pretende obter a validade jurídica da Nota Fiscal Eletrônica pela assinatura[viii] digital do remetente. Trata-se de um projeto inovador, cujo objetivo, em síntese, é gerar maior controle e cruzamento de dados das operações do contribuinte, bem como, simplificar suas obrigações acessórias, permitindo o ineficiente monitoramento[ix], em tempo real, das operações comerciais pelo Fisco.

O presente estudo visa demonstrar que o Projeto NF-E nasce em meio a um processo de avanço e sofisticação das pragas virtuais[x].O Brasil tem sido consagrado com o título de um dos países mais inseguros do mundo[xi]. O problema da corrupção é endêmico e deve ser levado em consideração nesta análise de risco de implantação da NF-E. Esta realidade enfraquece sistemas, distorce conceitos e encoraja pessoas a aplicar suas habilidades e tempo de maneira não produtiva. A Administração Fazendária Nacional deve estar consciente de que projetos desta natureza

irão conviver no mesmo ambiente onde reside um vertiginoso e alarmante crescimento do cibercrime, desde o início do século XXI. A especialidade destes criminosos é não deixar rastros, dificultando a detecção da fraude e criando novos desafios à Administração Fazendária, para definição de políticas efetivas de gestão de risco. Até o momento, o Projeto padece de análises e estudos mais aprofundados, para adoção de sistemas de segurança interna de fortalecimento das Administrações Fazendárias, bem como, treinamento de Auditores Fiscais de Rendas no Combate ao Cibercrime. Os Agentes Fazendários deverão estar treinados e dominar as novas tecnologias.

Tais dados deveriam suscitar grande preocupação de governantes e contribuintes, uma vez que persiste, até então, o anonimato e a sensação de impunidade[xii], como fator de estímulo à nova geração de cibercriminosos, acrescida da ineficácia legislativa e particularidade do Estado Brasileiro.

Recentemente, quadrilhas de cibercriminosos que atuavam junto a Receita Federal, na extração de certidões negativas de débitos fiscais, foram surpreendidas pela ação efetiva da Polícia Federal. Cerca de cem milhões de reais de certidões falsas foram retiradas. Trata-se de documento que tem característica similar à Nota Fiscal Eletrônica. Considerando este tenebroso cenário e ainda outras prerrogativas, recomendei a Federação das Indústrias do Estado de São Paulo a adoção de uma ação pró-ativa e participativa do Instituto Nacional de Criminalística da Polícia Federal no Projeto Nota Fiscal Eletrônica. O INC tem muito a oferecer, em termos de ações preventivas ao Estado-Cidadão-Arrecadador. Adota-se a expressão "Estado-Cidadão-Arrecadador", pelo fato do cibercrime, uma vez lançado, se propagar como uma onda nociva, que percorre a rede em uma velocidade incontrolável, atingindo uma cadeia indeterminável de contribuintes e cidadãos. Por seu lado, enfraquece a ação do Estado, cuja missão imprescindível, é tutelar e proteger o cidadão, ao mesmo tempo, que arrecada recursos para resguardar o bem comum. A experiência dos Bancos serve como pertinente amadurecimento e projeção do cibercrime. A NF-E incumbe-se do trânsito de valores pela internet, em larga escala, de documentos públicos. Futuramente pretende-se que o método de emissão seja puramente eletrônico, e a garantia e a validade jurídica da nota eletrônica seja resguardada pela assinatura digital, bem como, pela utilização de criptografia. Circula pela rede a comprovação da ocorrência de fatos geradores e a quitação de obrigações tributárias de grandes contribuintes em todo Brasil está ameaçada. Paira o risco ao Estado-Cidadão Arrecadador. O simples armazenamento inadequado[xiii] de senha ou mesmo extravio é de inteira responsabilidade do Contribuinte e coloca em risco o Projeto da Nota Fiscal Eletrônica. É uma corrida na qual a mesma história vem se repetindo: a cada solução inovada, surge um novo problema. Pesquisa conduzida pela IBM aponta **que 100% dos usuários** temem o cibercrime mais que delitos físicos. Relatório da IBM de 2006 prevê a evolução do Cyber Crime.[xiv]. O lucro faz o cibercrime se estabelecer mundialmente. A Legislação que trata do cibercrime não deve ser deficiente e o método de combate precisa ser pró-ativo. Acredito, assim como muitos, que é necessário ao legislador brasileiro, um tratamento especial na elaboração de normas mais claras e detalhadas, a fim de assegurar maior segurança jurídica e transparência aos contribuintes, assim como a efetiva punição dos criminosos. É emergencial a criação de armas preventivas, pró-ativas para agilizar a ação do Estado e o conseqüente beneficiamento dos contribuintes. O combate ao cibercrime só se apresenta pró-ativo em alguns, em outros é reativo. Vale citar como exemplo pró-ativo os casos de pedofilia, onde a Polícia Federal tem feito uma varredura na rede de grande importância para o combate desses crimes.

Até quando o Estado não tenha uma tradição ou legislação preventiva e pró-ativa para promover a defesa do Estado e dos contribuintes, o Cibercrime agirá livremente na adulteração proposital de Notas Fiscais Eletrônicas. E isto se dará por meio da criação de métodos que possibilitem a declaração de informações falsas, inserção de elementos inexatos, falsificação ou adulteração da nota fiscal de modo que ela tenha aparência de regularidade. A falta de uma metodologia, legislação específica e normatização que ampare métodos de investigação e auditoria é um fator a ser levado em consideração, uma vez que, grande parte da Fiscalização da Administração Fazendária não está treinada para coibir avançadas fraudes e simulações.

A exemplo da iniciativa privada, segundo a Federação Brasileira de Bancos - Febraban, a falta de uma legislação específica para crimes virtuais no Brasil é, hoje, uma forte barreira para o combate desse tipo de fraude. Também pela voz de Marcos da Costa; Diretor-Tesoureiro da OAB-SP e especialista em Direito de Informática: "Há situações novas que configuram os chamados crimes atípicos, que clamam por uma legislação própria, pois não se enquadram nos tipos penais em vigor".[xv] Por conta dessa lacuna, a Polícia Federal e a Justiça tratam esse tipo de delito pela legislação comum, o que dá margem as seguintes questões: Quais são as garantias ao contribuinte? Qual a segurança ao Estado-Cidadão-Arrecadador? Vamos deixar estas perguntas no ar para reflexão, até porque o projeto NF-E está em fase de testes e, para a adequação deste lamentável quadro, seriam necessárias significativas alterações das antigas e desatualizadas leis penais e processuais brasileiras. Não é outro o objetivo do amplo Projeto de Lei 89/2003 que, atualmente, tramita no Senado Federal.

Já no início de 2006, a imprensa anunciava: "A fraude virtual representa 80% da perda de bancos com roubo"[xvi]. Face ao grande volume de incidentes e forte impacto das fraudes eletrônicas sobre o setor bancário a Febraban defende que fraudes na internet passem a constar na legislação do país como crime inafiançável, pautando-se na premissa de que há falta de uma legislação específica capaz de punir de forma adequada o cibercriminoso no Brasil.

O crime virtual já é mais lucrativo do que o narcotráfico. A Secretaria da Fazenda de São Paulo publicou (Informativo CAT n° 63), comentando que o comércio ilegal se expande na Internet e a pirataria que o acompanha já apresenta números superiores ao narcotráfico. Portanto, não existe panorama otimista no tocante à utilização de transações de interesse público no ambiente eletrônico. Foi informado, ainda, que o Estado está impotente face ao crime organizado; o crime cibernético cresce e se consolida no mundo todo tirando proveito do avanço da tecnologia e da vulnerabilidade da comunicação.

III - Uma Administração Fazendária Forte com auxílio dos órgãos de combate ao cibercrime.

Um fisco forte, só será possível com a construção democrática de métodos de segurança, transparente na relação com os contribuintes. Um projeto pautado em dados e informações verossímeis. A função do Estado Democrático de Direito é a construção de um método preventivo e simultâneo de combate à corrupção e sonegação. Não li até o momento absolutamente nada sobre os sistemas de segurança que o Fisco pretende implementar para garantir que informações não sejam corrompidas ou "vazadas". Obviamente o cibercriminoso vai atacar o lado mais fraco da relação Fisco-Contribuinte.

Infelizmente o combate à corrupção no Brasil não costuma ser enumerado entre as missões da administração pública[xvii]. Ao meu ver, apenas um lado do tema tem sido enfrentado, mas precisamos trilhar todos os caminhos porque a corrupção e a fraude sempre encontram um atalho. Contudo a publicação do artigo de minha autoria no Portal Interestadual de Informações Fiscais é uma clara demonstração de que existe a preocupação de Administradores e Coordenadores Fazendários e o Fisco pede auxílio [xviii].

Dados oficiais apontam que, só no ano de 2005, os prejuízos com fraudes eletrônicas no mercado nacional ultrapassaram R$ 300 milhões [xix]. Contudo, estes números são muito superiores e determináveis.

Determináveis por dois motivos: o uso em larga escala dessas ferramentas sofisticadas de segurança dos Bancos envolve custos elevados. **Nenhum banco vai investir bilhões[xx] de reais em proteção mais do que perde com as fraudes. Para ilustrar, apenas** o Banco Itaú mantém investimento anual de cerca de R$ 1 bilhão em tecnologia da informação, sempre buscando oferecer **ainda mais segurança** e modernidade aos clientes. Bilionário investimento demonstra uma cifra de perdas do mesmo calão, para justificar o montante investido. A Febraban e as administradoras de cartão de crédito não divulgam o valor das perdas com fraudes por razões de segurança[xxi]. Os bancos não têm interesse de comunicar certos roubos para não perder a credibilidade frente aos correntistas e investidores. As tentativas de fraudes pela rede cresceram 579% em 2005. Até o final de 2006, as perspectivas no volume de perdas devem aumentar 20%[xxii].

Tomando o Estado como exemplo, os Bancos, considerando a bojuda perda e o bilionário investimento em segurança, pode-se meditar que a adoção de soluções de segurança tecnológica, somente pela parte da iniciativa privada, será suficiente. Seria como passar a responsabilidade do combate ao cibercrime somente à iniciativa privada. Levando-se em consideração a experiência dos bancos, reclama ao Estado maior cautela com a adoção de ferramentas tecnológicas que viabilizaria o trânsito de documentos públicos e adotar grandes investimentos[xxiii]. Órgão de abrangência nacional manifestou que o projeto da NF-E deve oferecer adequada infra-estrutura e robusto suporte tecnológico aos contribuintes.

Segundo Marcia Benedicto Ottoni [xxiv], a adesão à documentação exclusivamente eletrônica depende de uma infra-estrutura técnica e legal que normatize práticas que suportem as transações eletrônicas com técnicas eficientes de combate à insegurança, própria do meio digital – vulnerabilidade dos sistemas, instabilidade, impessoalidade e imateriabilidade dos registros – técnicas capazes de minimizar as fraudes e promover relações mais seguras. Durante esta transição, os advogados serão freqüentemente consultados sobre as conseqüências jurídicas de criar, receber, transmitir, destruir, registrar, guardar e converter cópias materiais em documentos eletrônicos.

O panorama sistêmico de riscos cibernéticos foi alvo de um amplo estudo realizado pela Deloitte com 150 organizações de um setor com alto grau de dependência tecnológica: as instituições financeiras. Formada em sua maioria (88%) por bancos e seguradoras, expressa visões e soluções de corporações de todo o mundo, inclusive o Brasil "[xxv]. Nas últimas duas edições da pesquisa, o acesso não autorizado a informações pessoais foi o item mais assinalado entre as preocupações relacionadas à **privacidade de dados: 84% em 2006 e 83% em 2005, contra 62% em 2004. (Grifei)** [xxvi]

Outro fator, a ser ponderado pela Administração Fazendária, seria para a velocidade de processamento, atualizações e agilidade dos fraudadores que utilizam programas maliciosos que se atualizam automaticamente [xxvii]. Além do Chile, não há notícia de países de primeiro mundo (Estados Unidos/Europa) que tenham adotado o sistema NF-E.

Curiosamente é mister mencionar que na América Latina, o Brasil não é integrante de um dos maiores acordos mundiais para desenvolvimento de segurança de ponta na Internet: Acordo de Wassenaar, firmado pelos integrantes do G7 e diversos paises. Tal tratado tem o objetivo de limitar a exportação da chamada tecnologia sensível aos países não signatários como o Brasil. Essa questão, voltada à Segurança Nacional Brasileira, não tem merecido maiores preocupações de alguns setores oficiais. A Argentina, é signatária do acordo, que também envolve a troca de informações para construção da criptografia de ponta com vista a impedir a ação de invasores e a ação de terroristas.

É justamente neste particular, que a atuação preventiva do governo deve ser efetiva: viabilizar à sociedade, o alcance de um patamar mais elevado de desenvolvimento, diminuindo, na medida do possível, as perdas de arrecadação que possam ocorrer. Torna-se imperiosa a necessidade de que se aprofundem os estudos sobre as garantias contra perdas e invasões dos contribuintes e a preservação da boa fé.

A utilização isolada da Nota Fiscal Eletrônica aponta para o fato de tornar-se um novo alvo de grande geração de riqueza ao cibercriminoso. Para as empresas, um novo fator de risco sistêmico de segurança corporativa, que certamente entrará em conflito com as leis internacionais, - *Sarbanes-Oxley*, - e outras que tratam do rígido controle interno de informações corporativas.

Redes de computadores são usadas todos os dias por corporações e várias outras organizações, portanto vulneráveis. Para piorar a insegurança do trânsito de documentos públicos no Brasil, não há regulamentação sobre provedores de Internet e suas responsabilidades. Eles atuam segundo seus próprios critérios, em geral, movidos por razões apenas econômicas. No Senado, entre outras propostas, tramita o projeto de lei 5.403/01, que regulamenta o acesso às informações na rede. Se aprovado, os provedores de Internet terão de arquivar por um ano o histórico de acesso de seus usuários para ajudar no combate ao uso indevido da rede[xxviii].

Neste sentido, para a implantação de um projeto desta magnitude, os Auditores Fiscais de Renda dos Estados, Municípios e da esfera federal, devem dominar as novas tecnologias, assim como os contribuintes.

IV - O bem tutelado é o Estado Cidadão Arrecadador e a ordem tributária Nacional[xxix].

As recentes mudanças no cenário econômico no planeta, decorrente do rápido crescimento do comércio eletrônico e a implementação no Brasil do trânsito de documentos públicos pela rede mundial de computadores merecem especial atenção. As formas de tributação serão afetadas pela velocidade do processo tecnológico, base da Nota Fiscal Eletrônica e do Sistema Público de Escrituração Digital.

As Fazendas Estaduais para promover o pretendido processo de "revolução fiscal" têm de passar por um processo de fortalecimento interno em vários níveis para depois, colocar em pauta o decisivo instrumento de integração da gestão tributária nacional em suas diferentes esferas. Neste sentido, para a implantação de um projeto desta magnitude, os Auditores Fiscais de Renda dos estados, municípios e da esfera federal, devem dominar plenamente as novas tecnologias, assim como os contribuintes. Len Hynds, chefe da luta contra os crimes da Internet na Inglaterra, diz que todo policial tem de dominar as novas tecnologias[xxx].

Do mesmo modo que a Nota Fiscal Eletrônica, quando o Emissor de Cupom Fiscal (ECF) foi criado, anunciava-se o fim das fraudes fiscais no varejo[xxxi]. Em um segundo momento, a partir de fraudes sistêmicas, parecer do Conselho Nacional de Política Fazendária anulou a validade de equipamentos anteriormente homologados. Restou comprometido, desta forma, o pilar básico de tal projeto, bem como, os requisitos específicos de segurança da informação e a comprovação eficiente da autenticidade e integridade. Estes pareceres "garantiam" a inviolabilidade[xxxii] das máquinas Emissoras de Cupom Fiscal, mas foi visto, que as armas da sonegação fiscal sempre encontram os seus caminhos. Por outro lado, a Polícia Federal concluiu que os meios eletrônicos[xxxiii] já são capazes de simular o efeito marca d'água, previsto do Convênio Confaz 10/05, este inclusive, ainda mais fácil de ser simulado de forma caseira, com o uso de tintas ou produtos químicos. O Estado de São Paulo, de forma excepcional, não aderiu a este Convênio, face à Informação Técnica do Instituto Nacional de Criminalística da Polícia Federal.

Ainda para a fase de implantação, coordenadores e administradores fazendários, devem trabalhar com a cooperação de técnicos fazendários especializados com altíssimo nível, bem como se valer da experiência do setor de combate aos crimes cibernéticos do Instituto Nacional de Criminalística da Polícia Federal.

Face ao exposto, deve-se estudar este projeto, visto que caminha sobre um dos piores cenários mundiais do cibercrime. Considerando que o iminente trânsito maciço de informações fiscais pela rede mundial de computadores é correto, a inteligência fiscal, deveria realizar uma análise de riscos pautada em parâmetros como em qualquer projeto. Tratar o projeto como inviolável ou infalível é um completo exagero e demonstra irresponsabilidade por parte de algumas empresas ditas como "provedoras de solução". Os que "vendem somente facilidade" devem mostrar, de forma isenta e profissional, o terreno em que estamos pisando.

Para que o Estado possa utilizar a Nota Fiscal Eletrônica e o Sistema Público de Escrituração Digital deve ter elevada disponibilidade de sistema, ou seja, ter um sistema "on-line" sete dias da semana. Ou seja, o sistema Fazendário Nacional e da Secretaria da Receita Federal têm que adotar um sistema de características especiais de segurança, monitorado vinte e quatro horas todos os dias, agregando técnicos e equipes multidisciplinares de plantão, assim como as empresas que emitem grande quantidade de documentos fiscais. O Ferramental técnico sequer foi preparado uma vez que pouco se investiu no projeto em termos de segurança da SRF e das Fazendas Estaduais.

Por outro lado, atualmente, nem os bancos têm um sistema de "back-up" e de disponibilidade de serviço 24 horas. Não porque os Bancos não possam ter este sistema, mas porque o custo é demasiado elevado sobrecarregando as instituições financeiras. Tente acessar o banco pela internet às 3 horas da manhã. Ademais, na hipótese de falhas a Fazenda e as empresas devem ter uma máquina "Hot-Sap", ou seja, quando uma máquina falhar, for invadida, ou vierem às contingências, os dados devem ser transferidos para outra máquina.

Apesar de ver com bons olhos o Projeto, está clara a percepção de que as administrações fiscais ainda não estão totalmente preparadas para promover de forma isolada a NF-E e o Sped. Prova disso é que problemas de controle simples fazem parte hoje do custo Brasil. Hoje a empresa multinacional de escol sofre um elevado "peso" operacional como a simples retirada de uma Certidão Negativa de Débito[xxxiv]. Ou seja, uma simples Certidão[xxxv] de regularidade fiscal, na atualidade, ainda é fator de entrave ao ambiente de negócios no Brasil e via reflexa, para a baixa competitividade internacional[xxxvi]. O controle de débito Fiscal da União, Estado ou Município aponta débito inexistente, ou mesmo, em valor inferior âquele devido. Minha conclusão ainda se apóia na recente manifestação de organismos internacionais como a Organização para a Cooperação e o Desenvolvimento Econômico (OCDE) e a Organização Mundial de Comércio (OMC), que diante das perdas potenciais de receitas tributárias resultantes do desenvolvimento do comércio eletrônico, sugeriram uma "Política Fiscal Mundial" para a tributação desse tipo de comércio. A amplitude mundial dessa "política fiscal" se faz necessária, uma vez que não há mais limites territoriais às operações comerciais, em razão dos avanços tecnológicos, tais como a internet e a virtualidade das transações[xxxvii]. Essa mesma política fiscal deverá ser implantada em relação ao cibercrime.

Pesquisa recente envolvendo duzentos contabilistas e consultores e profissionais da área financeira de pequenas, médias e grandes empresas foi realizado durante uma palestra de um renomado Centro de Estudos em São Paulo. Na oportunidade foi questionado se algum dos profissionais presentes acreditava no projeto NF-E, bem como, foi perguntado se as pesquisas de aceitação da Nota Fiscal Eletrônica traduzem a realidade. Todas as duzentas pessoas presentes informaram que não acreditam na NF-E. Na ocasião apontaram o receio de falhas tecnológicas[xxxviii] em massa, bem como, temiam pela forma como o projeto estava sendo veiculado na mídia.

Com relação às notas fiscais e escrituração preenchidas via Internet, pode-se prever o mesmo perigo[xxxix] ao estado e contribuintes, uma vez que a especialidade do cibercriminoso é quebrar códigos e cometer fraudes. Especialistas explicam que o grampo de Internet, visando a clonagem de Notas Fiscais Eletrônicas, é tão possível quanto o telefônico, bastando possuir tecnologia para tal, o que não é muito difícil.

A Nota Fiscal Eletrônica teria sido criada como um caminho para a Reforma Tributária e posterior unificação de impostos, criando-se o imposto único não cumulativo. O Informativo CAT n° 64[xl] faz referência à Europa, berço deste imposto, que sofre fraudes generalizadas envolvendo operações intercomunitárias. A Comissão Européia criou uma equipe de especialistas de alto nível para examinar a situação e propor alternativas.

V –Conclusão

É claro que o monitoramento eletrônico de operações melhorará, e muito, a eficácia da ação fiscal, mas outras janelas de sonegação sempre existirão. A Nota Fiscal Eletrônica é uma realidade a ser estudada com cuidado e ponderação pelas autoridades. Este documento digital é um sistema que precisa ser acompanhado de perto pelo Instituto Nacional de Criminalística da Polícia Federal e Ministério Público, de forma ampla e completa. O provável é o caminho que leva para a certeza.

O crime na Internet e a impunidade tornaram-se um círculo vicioso que, sob o ponto de vista tecnológico, parece não ter limites. "Nós criamos uma civilização global em que elementos cruciais - como as comunicações, o comércio, a educação e até a instituição democrática do voto - dependem profundamente da ciência e da tecnologia. Também criamos uma ordem em que quase ninguém compreende a ciência e a tecnologia. É uma receita para o desastre. Podemos escapar ilesos por algum tempo, porém, mais cedo ou mais tarde, essa mistura inflamável de ignorância e poder vai explodir na nossa cara". (Carl Segan).

Referências

[i] Artigo: NF eletrônica em fase operacional. **Fonte**: Informativo CAT – Ed. nº 65 de agosto de 2006. Publicação mensal interna do Conselho Superior da Coordenadoria da Administração Tributária da Secretaria de Estado dos Negócios da Fazenda do Estado de São Paulo.

[ii] Artigo: Salve-se dos hackers quem puder. Francisco Camargo - Presidente da CLM Software. Comento que, pela doutrina moderna, o correto seria *cracker*. Fonte: Gazeta Mercantil de 29 de agosto de 2006. Caderno A – p. 3.

[iii] Artigo - Por Matthew Jones, da Reuters,- Cibercrime está se tornando mais organiza do Sexta-feira, 15 de setembro de 2006 - 14h35 LONDRES (Reuters). Fonte: Website :http://info.abril.uol.com.br/aberto/infonews/092006/15092006-7.shl.

[iv] Artigo de Christopher Painter, vice-diretor da seção de crimes eletrônicos e de propriedade intelectual do Departamento de Justiça dos EUA, 22/09/2006, 19:22,Fonte:Módulo,Security,News http://wnews.uol.com.br/site/noticias/materia.php?id_secao=4&id_conteudo=5988

[v] Revista, Deloitte de setembro de 2.006.

[vi] Conforme retrata o informativo CAT (com as ressalvas da nota de n°1), edição de outubro de 2.006.

[vii] O teatro das idéias/Shaw,Bernard, 1856,-1.850; organização Daniel Pizza; Tradução José Viegas Filho.- São Paulo: Companhia das Letras, 1996, pág.51.

[viii] Artigo do Prof. Pedro Antonio Dourado de Rezende, Depto. de Ciência da Computação, Universidade de Brasília 7 de Outubro de 2003, Privacidade e Riscos num mundo de chaves públicas, Relatório sobre o tema "Privacidade e Responsabilidades na Infra-estrutura de Chaves Públicas ICP-BR" ,I Fórum sobre Segurança, Privacidade e Certificação Digital ITI -Casa Civil da Presidência da República, Fonte: http://www.cic.unb.br/docentes/pedro/trabs/forumiti.htm

[ix] Artigo Publicado no jornal Valor Econômico dia 03.08.05, pelo ex. Coordenador da Administração Tributária. O monitoramento eletrônico melhorará em muito a eficácia da ação fiscal, mas outras janelas de sonegação existirão.

[x] Salve-se quem puder! Caos pode imperar na segurança virtual, autor, Francisco Camargo é presidente da CLM Software, distribuidora de soluções de segurança.
Artigo publicado no *Website* da ABES – Associação Brasileira das Empresas de Software http://www.abes.org.br/templ1.aspx?id=269&sub=269

[xi] Françoise Terzian. Reportagem do caderno tecnologia de 24.08.2006. Sua identidade digital corre perigo. As fraudes on-line não param de crescer - e o Brasil é um dos países mais inseguros do mundo. Fonte: http://portalexame.abril.com.br/revista/exame/edicoes/0875/tecnologia/m0101272.html

[xii] Fonte: Artigo publicado na Gazeta Mercantil na data de 20 de setembro de 2005 de autoria do advogado Marco Wadhy Rebehy do escritório Portugal & Rebehy Advogados.

[xiii] Armazenamento inadequado põe em risco a segurança da nota fiscal eletrônica, matéria de Jackeline Carvalho, no Website, Convergência Digital de 10.07.2006, fonte: http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=3691&sid=3
xiv Para ler a notícia, basta clicar no link abaixo: http://tecnologia.terra.com.br/interna/0,,OI848630-EI4805,00.html
xv Fonte: Matéria de Capa do Jornal do Advogado da OAB-SP Nº 306 / maio de 2006.

[xvi] Gazeta Mercantil - 11/01/06 P.C1.
[xvii] Este foi o comentário do Agente Fiscal de Rendas da Secretaria da Fazenda do Estado de São Paulo e jornalista especializado em Políticas Públicas pela Faculdade Latin-Americana de Ciências Sociais de Buenos Aires, Hideyo Saito, recomendo o excelente artigo publicado na revista Plenafisco pág 26.
[xviii] Artigo: Certificação Digital e Segurança. In: E-dicas: o direito na sociedade da informação. Marcia Benedicto Ottoni. Gerente Jurídica da CertiSign.

[xix] Matéria - Tatiana Schnoor - 21.03.2006
http://wnews.uol.com.br/site/noticias/materia.php?id_secao=4&id_conteudo=4148
xx Fonte: http://www.cert.br/stats/incidentes/ Estatísticas dos Incidentes Reportados ao CERT.Br.

[xxi]
Fonte:http://wnews.uol.com.br/site/noticias/materia.php?id_secao=4&id_conteudo=4148

[xxii] Fonte: http://www.cert.br/stats/incidentes/ Estatísticas dos Incidentes Reportados ao CERT.Br.
[xxiii] http://www.fazenda.sp.gov.br/
[xxiv] Artigo: Certificação Digital e Segurança. In: E-dicas: o direito na sociedade da informação. Marcia Benedicto Ottoni. Gerente Jurídica da CertiSign.

[xxv] Revista Mundo Corporativo nº 13, 3º Trimestre 2006-09-15, Artigo, ACESSO RESTRITO
[xxvi] Idem 22, Revista, Deloitte de setembro de 2.006 - O panorama sistêmico de riscos cibernéticos foi alvo de um amplo estudo realizado pela Deloitte com 150 organizações de um setor com alto grau de dependência tecnológica (....).

[xxvii]
Fonte:http://wnews.uol.com.br/site/noticias/materia.php?id_secao=4&id_conteudo=4148

[xxviii] Criminosos cibernéticos. Matéria de Capa do Jornal do Advogado da OAB/SP Nº 306 / Maio de 2006 /Bandidos.com, informando que cada vez mais, bandidos roubam informações e lesam via internet.

[xxix] "Cabe ao Fisco garantir a autenticidade e segurança da Nota Fiscal Eletrônica" Publicado na Data de 27/07/2006 no Website jurídico Migalhas, endereço http://www.migalhas.com.br/mostra_noticia_articuladas.aspx?cod=27933
Artigo/Comentários/a/NotaFiscal-Eletrônica,endereço:-http://www.migalhas.com.br/mostra_noticia.aspx?op=true&cod=27211, publicado em 11/07/2006
[xxx] CAPA DA VEJA São Paulo, 3.11.04 e posterior reportagem.
[xxxi] Estudos que realizei junto a especialistas e pesquisas de campo. Estes artigos foram publicados no "Website" do Portal Jurídico "Migalhas" e no "Website", Portal Interestadual de Informações Fiscais.
[xxxii] www.abraform.org.br/news/abraform%20NEWS%20maio.pdf
[xxxiii] Conforme concluiu a informação de n° 71/05, subscrito pela Diretoria Técnico Científica do Instituto Nacional de Criminalística da Polícia Federal, artigo do autor, Facilitadores da Evasão Fiscal, comentários publicados pela Associação Paulista dos Magistrados no endereço: http://www.apamagis-lex.com.br.
[xxxiv] Na data de 22 de setembro na AMCHAM acorre um movimento Nacional sobre o tema: Portal e Website, jurídico Migalhas, "As múltiplas visões sobre a Nota Fiscal Eletrônica e o Sistema Público de Escrituração Digital" http://www.migalhas.com.br/mostra_noticia_articuladas.aspx?cod=30519.

[xxxv] Certidão Negativa de Débitos visa a demonstrar quais débitos o contribuinte tem para com o Fisco ou quais débitos estão em aberto, mas com as garantias depositadas em juízo ou oferecidas ao Estado para serem penhoradas. Sobre a burocracia Brasileira e a falta de estrutura para ambiente de controle adequado veja a Carta da Câmara Americana de Comercio Para o Brasil, maior entidade multisetorial da América-Latina

http://www.amcham.com.br/update/update2006-04-25c_dtml.pdf#search=22AMCHAM20CND%22

[xxxvi] É imensa a dificuldade em obter-se a tal da CND, que está associada a duas outras pedras duras do ambiente de negócios no Brasil. Uma, a elevada carga tributária direta, com mais impostos do que os empresários podem pagar. Outra, a custosa carga tributária indireta, com mais burocracia do que as empresas podem agüentar. Fonte: http://www.amcham.com.br/update/opiniao/opiniao2006-05-23d

[xxxvii] Revista Pleafisco, Gramado/RS, Edição n° 3 de agosto de 2.006, página 28 e 29.

[xxxviii] Fonte: Revista Info, abril de 2006.

[xxxix] Esse foi o comentário de Fabio Bastiglia Oliva - Diretor da Safe Networks.

[xl] Trata-se de informativo mensal da Coordenadoria da Administração Tributária da Secretaria da Fazenda do Estado de São Paulo, que objetiva informar o Auditor Fiscal de Rendas e os Juízes do Egrégio Tribunal de Impostos e Taxas da Secretaria dos Negócios da Fazenda do Estado de São Paulo, conforme descrito na nota de n°1.

[*] **Coriolano Aurélio de Almeida Camargo Santos, sócio Diretor da Almeida Camargo Advogados é advogado militante, com dezoito anos de vivência na área jurídica. Nomeado por Decreto do Sr. Governador do Estado de São Paulo, atualmente exerce o cargo de Juiz da Quarta Câmara Efetiva do Egrégio Tribunal de Impostos e Taxas da Secretaria da Fazenda do Estado de São Paulo (1935). Membro do Grupo de Estudos Tributários – da Federação das Indústrias do Estado de São Paulo - FIESP. Membro convidado da Comissão de Estudos da Concorrência e Regulação Econômica - CECORE da OAB/SP, onde atualmente participa de seu grupo de estudos tributários. Membro Consultor da Comissão OAB vai a faculdade. Nomeado pelo Presidente da Ordem dos Advogados do Brasil, Secção São Paulo, - Portaria de N° 482/06/PR-, como integrante efetivo da Comissão do Cooperativismo da OAB/SP. Membro do Comitê de Estudos relativos ao desenvolvimento de políticas ambientais do Encontro de Meio Ambiente do Vale do Paraíba. Membro da Delegação Organizadora do Ecovale - evento, sem fins lucrativos, idealizado e organizado pelo Sindicato dos Engenheiros no Estado de São Paulo, SEESP. Membro do Grupo de Estudos sobre o Sistema Público de Escrituração Digital e Nota Fiscal Eletrônica. Teve vários artigos e trabalhos publicados e revistas especializadas e jornais.**

Garantia de Políticas de Privacidade utilizando-se Certificação Digital

R. A. Gotardo, R. A. Rios, R. E. Grande, S. D. Zorzo, *Universidade Federal de São Carlos - S.P.*

Abstract — **The Brazilian legislation does not protect completely the privacy of the Web user. The issues of user privacy at the Internet access are considered introducing an architecture to guarantee information security. This architecture provides tools to warrant that the privacy policies have juridical legitimacy. This judicial quality is reached by the description of such policies in the format of P3P protocol, the checking of these policies using privacy seals and the authentication of the seal by means of digital certificates.**

Index Terms — **Internet, Privacidade, Personalização, Segurança.**

I. Introdução

O conhecimento humano é, atualmente, o principal capital da sociedade contemporânea, a chamada "sociedade da informação".

A informação é a base geradora ou transformadora do conhecimento. Portanto, é objeto de preocupação a proteção e a manutenção desta para que sua utilização seja eficiente e segura. Isto insere também a necessidade de reformulação de conceitos, busca por novos métodos e princípios que tentarão equilibrar as relações entre indivíduos dessa sociedade, considerando que, na maioria dos casos, as informações são a respeito de pessoas, sejam estas clientes, usuários, parceiros, etc. [23]

As informações pessoais requerem proteção jurídica para que não sejam utilizadas de forma indevida ou de forma não autorizada. Essa proteção também evita prejuízos significativos e danos das mais variadas formas. Neste intuito, vários movimentos pelo mundo e no Brasil incitam a defesa da privacidade.

Muitos autores citam que privacidade é um direito defendido em nossa Constituição Federal, assegurado por nossos Códigos (notadamente o Civil, o Penal, o de Defesa do Consumidor e o Comercial) e protegido por leis esparsas. Contudo, surpreende o fato da palavra privacidade não aparecer em nossa Constituição, não constar em nossos Códigos e nem ser citada pelas mencionadas leis [20].

Um conceito de privacidade amplamente difundido é que "Privacidade é o direito de estar sozinho". Além desta afirmação tem-se "O direito à privacidade termina com a divulgação de fatos pelo indivíduo ou com o seu consentimento".

Identifica-se, então, um cuidado que cada um deve ter em proteger sua privacidade, pois, uma vez que alguém divulgue ou autorize a divulgação de um fato ou informação pessoal, não há como reverter a situação [17].

Pode-se resumir grande parte dos problemas associados à privacidade do indivíduo como sendo a manipulação de informações pessoais sem autorização ou conhecimento do mesmo.

No Direito, é possível constatar que a questão da privacidade alcança várias esferas, seja Civil, Administrativa ou Penal.

Dentro destas esferas, surge a necessidade de leis que sejam relacionadas à proteção da privacidade.

No Brasil não há legislação específica, mas a manutenção da privacidade e a sua violação encontram subsídios em princípios garantidos em Códigos como o Penal, o Civil e o de Defesa do Consumidor [13].

Além de legislação específica, é necessária a regulamentação dos serviços e práticas que possam violar a privacidade das pessoas. Esse processo objetiva não só punir, como também coibir, agindo de forma ostensiva, evitando a violação da privacidade.

Existem maneiras de garantir ao usuário a proteção de sua privacidade nos mais diversos meios. Dentre estas, os chamados "Selos de Privacidade" regulam as políticas de privacidade dos sites da internet. Porém, também existem formas de confundir ou enganar o usuário, cuja confiança depositada em determinado site esteja sendo subvertida pela violação de sua privacidade.

O objetivo deste trabalho será relacionar práticas de violação e de defesa da privacidade do usuário na internet à legislação existente no Brasil, demonstrando a importância da regulamentação para coibição das práticas ilegais e garantias de melhor utilização das informações dos usuários. Neste mesmo intuito, propor-se-á uma infra-estrutura, objetivando legalizar as políticas de privacidade descritas pelos sites, assegurando ao usuário uma legítima sensação de segurança enquanto navega por estes sites.

Este trabalho foi apoiado em parte pela CAPES (Brasil).

R. A. Gotardo, Departamento de Ciência da Computação da Universidade Federal de São Carlos e CAPES (e-mail: reginaldo_gotardo@dc.ufscar.br).

R. A. Rios, Departamento de Ciência da Computação da Universidade Federal de São Carlos e CAPES (e-mail: ricardo_rios@dc.ufscar.br).

R. E. Grande, Departamento de Ciência da Computação da Universidade Federal de São Carlos e CAPES (e-mail: robson_grande@dc.ufscar.br).

S. D. Zorzo, Departamento de Ciência da Computação da Universidade Federal de São Carlos (e-mail: zorzo@dc.ufscar.br).

II. LEGISLAÇÃO

A privacidade dos usuários da internet no Brasil vem ganhando cada vez mais importância com diversos trabalhos publicados a respeito.

Apesar de no Brasil não existir lei específica sobre a proteção à privacidade, há tipificações incluindo crimes que atentam contra a privacidade das pessoas. Na câmara dos deputados há um Projeto de Lei específica sobre privacidade (P.L. n.o 3.360/00), mas ainda não integra as regulamentações a respeito do assunto, nem inclui a criação ou definição de órgão de defesa e normatização dos serviços que lidam com informações dos usuários. A proposta deveria estabelecer uma multa maior do que aquela que foi submetida à apreciação, oscilando entre trezentos reais a um mil reais.

O primeiro princípio de proteção à privacidade está contido no artigo 5º da Constituição Federal do Brasil, onde se afirma que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". Como já mencionado, não há a palavra privacidade em nenhuma parte da nossa Constituição, porém, entende-se que a violação da vida privada e da intimidade atente contra o princípio da privacidade [13].

Segundo o Artigo 159 do Código Civil Brasileiro "todo aquele que, por ação ou omissão voluntária, negligência, ou imprudência, violar direito, ou causar prejuízo a outrem, fica obrigado a reparar o dano". Desta forma, considerando-se que a violação da privacidade de alguém poderá causar-lhe dano, ao autor caberá a reparação.

De acordo o artigo 6º do Código de Defesa do Consumidor, "são direitos básicos do consumidor a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços". Assim, mesmo não definida lei específica, ao consumidor é assegurada a proteção contra práticas abusivas. Nestas práticas, mecanismos colhem informações dos usuários que são utilizadas de forma ilegal ou sem consentimento do mesmo. Ainda neste artigo, é garantido ao consumidor "a efetiva prevenção e reparação de danos patrimoniais e morais, individuais e coletivos" (inciso VI).

A. Mecanismos de personalização que violam a privacidade na Web

Alguns mecanismos de coleta de informações são os *Cookies*, os *Web Bugs* e o *Clickstream*. Estes mecanismos são chamados de coleta implícita, pois muitas vezes os usuários não têm conhecimento do funcionamento destes ou não são informados sobre isto. Existem também mecanismos explícitos de coleta, como formulários para preenchimento, não só de dados pessoais, mas também de informações sobre preferências do usuário. O *Data Mining*, é um mecanismo de análise de informações coletadas, sejam estas explícitas ou implícitas.

Esta análise pode, em alguns casos, gerar novas informações, incoerentes ou incorretas. Isto pode caracterizar difamação (prevista no Código Penal no artigo 139) ou injúria (Código Penal, artigo 140) caso o método de análise destas informações falhe ao inferir resultados incorretos, imprecisos ou incoerentes.

Um exemplo disto seria um usuário que acessa um site de vendas de livros, procurando sempre por livros relacionados à doenças, como a Aids. Uma falha no mecanismo do *Data Mining* poderia concluir que o usuário é uma pessoa portadora do vírus HIV, acarretando prejuízos à pessoa que pode sofrer preconceitos caso estas informações sejam divulgadas.

O principal objetivo dos *Cookies* é a manutenção da sessão do usuário quando acessa algum *Web* site, porém insere informações no computador do usuário e depois se vale delas, freqüentemente, sem seu consentimento. Os *Web Bugs* tem como objetivo verificar se determinado usuário acessou algum artefato da *Web*. Estes dispositivos são importantes para a criação de perfis de usuários, controles estatísticos e, posteriormente, envio de formas de propaganda, que podem ser caracterizadas como *Spam*.

A função do *Clickstream* é a criação de perfis de usuários com base na sua navegação entre as páginas da *Web*.

Violam, assim, o artigo 5º, inciso X da Constituição Federal do Brasil bem como o Código de Defesa do Consumidor em seu artigo 43, parágrafo 2º, além de seu caput – defendendo o acesso às informações dos consumidores e que a abertura de cadastro, registro e dados pessoais e de consumo (principalmente) devem ser comunicadas ao consumidor por escrito, caso não solicitadas por ele. Ainda neste artigo, no 3º parágrafo, ao consumidor é assegurado o direito de corrigir estes dados quando julgá-los incorretos ou incoerentes.

Continuando no Código de Defesa do Consumidor, no artigo 53, onde legisla sobre o que é o Contrato de Adesão e que limitações de direitos devem ser redigidas com destaque. Verifica-se, desta forma, a existência de artigos que garantam o direito à privacidade das informações dos usuários, do acesso destes a estas informações e da punição em caso de violação destes direitos, mesmo que indiretamente [20] [21].

O *Spam* é uma forma de correspondência indesejada. O direito da vida íntima, ou seja, o direito à privacidade também inclui o direito de ser deixado só. Logo, o *Spam* caracteriza uma violação da privacidade das pessoas. Viola o artigo 5º, inciso X da Constituição Federal do Brasil; o artigo 6º do Código de Defesa do Consumidor, onde versa sobre práticas de propaganda enganosa e abusiva; os artigos 146, 147, 265 e 266 do Código Penal; bem como o artigo 65 da Lei de Contravenções Penais [20].

Os artigos 146 e 147 do Código Penal tratam do constrangimento ilegal e ameaça, respectivamente, pois, através do *Spam*, pode-se constranger alguém por grave ameaça a fazer algo ilegal ou deixar de fazer algo legal. Também é possível ameaçar pessoas com o uso do *Spam*, utilizando-se de informações enganosas.

Já os artigos 265 e 266 do Código Penal versam sobre

"atentado contra a segurança de serviço de utilidade pública" e a "interrupção ou perturbação de serviço telegráfico ou telefônico", perfeitamente cabíveis, considerando a internet um serviço de utilidade pública (talvez o maior deles em abrangência) e, muitas vezes, com infra-estrutura dependente dos serviços telefônicos.

O artigo 65 da Lei de Contravenções Penais refere-se a "molestar alguém ou perturbar-lhe a tranqüilidade, por acinte ou por motivo reprovável", onde o *Spam* enquadra-se muito bem como motivo reprovável.

Também existem práticas utilizando *Web Bugs* onde sites terceiros podem ser informados sobre a comunicação dos usuários com o site original.

B. *Garantindo sua própria privacidade na Web*

Existem mecanismos ou ferramentas que visam à garantia da privacidade dos usuários. Garantia esta prevista na Constituição Federal do Brasil. Sendo assim, são formas de proteger um direito pessoal e que, apenas por isto, não deveriam violar nenhuma lei. Porém, como contradições podem ocorrer no ordenamento jurídico, tratar-se-á aqui sobre a legalidade destes mecanismos.

1) A Criptografia: A criptografia é uma forma de "disfarçar" informações de acordo com um algoritmo e protegê-las por uma chave única e dificilmente decifrável.

Como todo cidadão tem o direito de expressar-se e sua comunicação não pode ser interceptada, a criptografia apresenta-se como um mecanismo legal.

No artigo 5º, inciso XII é assegurada a inviolabilidade do sigilo da correspondência e outros tipos de comunicações (onde se incluem as de dados), salvo por ordem judicial ou para investigação criminal ou instrução penal em formas estabelecidas por lei. Sendo assim, a criptografia não pode ser considerada ilegal, pois não há lei que impeça seu uso nas comunicações, mesmo havendo lei que possibilite a interceptação de comunicações, por meio de ordem judicial, estando esta criptografada ou não [21].

2) Agente de Privacidade e Filtros: Agentes de privacidade são programas "inteligentes" que informam aos usuários a respeito da violação de sua privacidade enquanto navegam pelos sites da *Web*.

Filtros são ferramentas seletivas que podem bloquear e-mails, páginas *Web*, *Cookies*, propagandas, *JavaScript* e outros conteúdos.

Como são ferramentas para o usuário manter o controle de sua privacidade não possuem restrições legais.

3) Anonimato, Pseudônimos e Máscaras: A palavra anonimato, derivada do latim *anonymus* (sem nome, sem assinatura), é a forma de navegação por sites de *Web* onde o usuário utiliza algum mecanismo para que sua identidade não seja revelada. Por identidade, considera-se o número do IP (*Internet Protocol*) de sua máquina, que poderia, mediante investigação, levar à identificação do usuário.

No artigo 5º, inciso IV, da Constituição Federal é respeitada a manifestação do pensamento com veto ao anonimato. Porém, nada é afirmado sobre o anonimato de trânsito, ou seja, na manifestação do pensamento é necessária a identificação de seu autor, porém, ao locomover-se pelas ruas, ao entrar em lojas, restaurantes, ou ao navegar na internet não há obrigatoriedade de identificação do usuário. Não sem o consentimento do mesmo.

E, como no inciso II deste mesmo artigo, "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei", a utilização de mecanismos que tornem a navegação dos usuários pela internet anônima não é ilegal.

Os Pseudônimos são melhorias no anonimato, garantindo melhor personalização dos serviços oferecidos ao usuário.

Com o uso do anonimato, um site não pode identificar os usuários a cada visita e, assim, não pode propor personalização de seus serviços.

O conceito de máscara [24] reflete o modelo da personalidade pública do indivíduo. Uma espécie de interface entre o indivíduo e a interação (comunicação) com o meio social.

Ishitani [8] utiliza esse conceito para construção de um sistema de navegação anônimo denominado MASKS. Este sistema é uma versão melhorada de pseudônimos e garante melhor personalização para os usuários, sem prejudicar sua privacidade, buscando um equilíbrio entre os dois.

Nenhum deles possui impedimentos legais, estando relacionados ao comportamento social do indivíduo e não constituindo crime de falsidade documental (Código Penal, artigos 296 até 305) e nem crime de falsa identidade (artigos 307 e 308) quando tratar-se de trânsito do indivíduo e em defesa da sua privacidade.

III. POLÍTICAS DE PRIVACIDADE

As políticas de privacidade dos sites da *Web* são documentos descrevendo a importância dada por uma determinada entidade (seja pessoa física, jurídica ou o próprio governo) à privacidade de quem está utilizando o site. Neste documento, são detalhadas informações sobre a coleta dos dados (quais mecanismos utilizados) e sobre o destino destes mesmos.

O maior objetivo das Políticas de Privacidade é aumentar a sensação de segurança dos usuários. Também, desta forma, as políticas de privacidade são atividades de Marketing [10].

Legalmente, não havendo regulamentação destas políticas não poderão ser consideradas válidas.

Para que os usuários não tenham que ler toda a política de privacidade em cada site visitado, escolhendo o que melhor lhe convier, foi criado o conceito de protocolos de negociação, através dos quais são automatizadas tais políticas e, assim, ferramentas podem ser criadas para leitura e análise automáticas.

A. *Protocolos de Negociação - a P3P*

A Plataforma para Preferências de Privacidade (P3P - *Plataform for Privacy Preferences*) é uma tentativa de padronização de protocolo de negociação e permite a negociação do usuário com o site, desenvolvida pelo Consócio

da *World Wide Web*.

É um conjunto de especificações sobre práticas de coleta e uso da informação por uma organização e visam assegurar ao usuário a garantia de não ter sua privacidade prejudicada ao acessar serviço disponibilizado por algum site na *Web*.

A P3P possibilita que agentes do usuário avaliem as políticas de privacidade de um site, desde que elas estejam disponíveis no formato estabelecido pela proposta.

A P3P pode ser considerada um complemento e um mecanismo de reforço às leis e aos programas de auto-regulamentação [34].

O protocolo introduzido pela Plataforma 3P é projetado em um formato XML, conhecido como política P3P de privacidade.

A P3P pode ser implementada pelos sites *Web* em seus servidores através da tradução de suas políticas de privacidade escritas numa linguagem humana para a sintaxe P3P. No final cria-se um ou mais arquivos-textos que contém suas políticas de privacidade traduzidas para essa sintaxe no formato XML.

Depois de publicar esses arquivos resultantes, um arquivo de referência da política é publicado junto desta para indicar quais partes do site a política será aplicada. Para auxiliar os operadores a desempenhar a tradução das políticas de privacidade para um formato padrão, existem diversas ferramentas automáticas.

Alguns aplicativos de navegação na *Web* já oferecem mecanismos para a leitura de políticas de privacidades dos sites, desde que estejam no formato P3P.

IV. SELOS DE PRIVACIDADE E CERTIFICAÇÃO DIGITAL

Um Selo de Privacidade é fornecido por uma empresa independente que verifica em uma página da *Web* as políticas de privacidade, a maneira como os dados pessoais são coletados, processados e compartilhados [10]. Com isso, sempre que um usuário entrar em um site o qual exibe um Selo de Privacidade, saberá que a entidade emissora de tal selo verifica periodicamente esse sistema *Web*. Esta verificação é realizada para que as informações contidas nas políticas de privacidade sejam respeitadas e a manipulação dos dados pessoais de um usuário não viole sua confiança.

Desta forma, os Selos de Privacidade são afirmações positivas a respeito das políticas de privacidade de um site.

Os Selos de Privacidade começaram a ser desenvolvidos com o objetivo de acompanhar o forte crescimento das vendas de produtos pela internet e, assim, tiveram o seu conceito intrinsecamente ligado à definição de B2C (*Business-to-Commerce*). As Empresas de comércio eletrônico sentiram a necessidade de aumentar a confiança dos usuários que visitavam seus *Web* Sites e garantir que os dados de cada cliente fossem mantidos de forma segura e confidencial.

Assim, a confiança dos consumidores tornou-se um fator de grande relevância para a estratégia das empresas de comércio eletrônico [15].

Além de garantir ao usuário que seus dados serão respeitados de acordo com as informações contidas na política de privacidade, os Selos de Privacidade permitem, ainda, por intermédio das coletas e análises dos dados, diferenciar cada cliente. Tornou-se possível traçar um perfil dos usuários, que deixaram de ser anônimos, baseando-se no histórico de acesso. A personalização de sites *Web* não serviu apenas para oferecer aos usuários produtos que eram de seu interesse, mas também se tornou um grande utilitário das empresas que passaram a oferecer produtos diferenciados, limitando as ofertas de acordo com o perfil e influenciando as intenções de cada cliente [10]. Aproveitando-se da aceitabilidade dos Selos por parte dos usuários, as empresas passaram a usar este mecanismo como uma solução baseada no Marketing [10] e obtiveram um tratamento diferenciado em relação às concorrentes que não ofereciam este recurso.

Existem diversas entidades que emitem Selos de Privacidade, mas as três mais proeminentes são *TRUSTe*, *WebTrust* e *BBBOnline* [12]. Mesmo com um grande número de entidades, existem requisitos padrões que são exigidos por todas, como a escrita de uma política de privacidade e uma garantia de que os dados armazenados estarão seguros. A segurança das informações é extremamente relevante, pois informações que estão desprotegidas não podem ser consideradas privadas, existindo assim uma estreita relação entre privacidade e segurança [12].

O uso de Selos de Privacidade tem sido criticado principalmente porque poucos sites comerciais possuem alguma declaração de privacidade. E, entre os sites que adotam esse sistema, existem casos de abusos no uso ilegítimo dos Selos de Privacidade.

Outra crítica é que usuários não entendem completamente a forma ou função dos Selos de Privacidade, poucos podem reconhecer um selo como verdadeiro e poucos deles reconhecem como uma ferramenta importante na decisão para confiar em sites *Web*.

Apesar destes dados negativos, os usuários da *Web* estão começando a reconhecer os Selos de Privacidade e seu significado. *Cheskin Research* reportou que 69% dos usuários *Web* reconheceram o selo da *TRUSTe* e 37% o selo da *BBBOnline* [14]. O selo da *TRUSTe* aumentou a confiança em um site *Web* para 55% segundo esta mesma pesquisa. Esse sucesso tem origem no aumento de adoção dos Selos pelos sites.

Os fatos e resultados de pesquisas mostram que há muito a ser explorado nesse contexto para melhorar algumas características e levar a uma maior adoção destas práticas.

O Certificado Digital é um documento eletrônico especificado pelo padrão internacional X509 que tem como principal objetivo associar chaves públicas às diversas informações de uma entidade [4].

Os certificados digitais são enviados sempre que o servidor necessite criptografar as informações contidas em uma requisição, ou quando for necessário reconhecer a identidade de uma entidade.

A Certificação Digital pode ser definida como um conjunto de técnicas para fornecer segurança às comunicações e às transações eletrônicas [18].

Um dos grandes benefícios trazidos pelo uso de Certificação Digital é a possibilidade de disponibilização de serviços fáceis de acessar, com maior agilidade e custos reduzidos [19].

O que torna um certificado digital confiável é a assinatura e a identificação da entidade que o emitiu. Para ter a sua validade garantida, os certificados devem ser emitidos por uma Autoridade Certificadora (CA - *Certificate Authority*) [3].

As principais características de um Certificado Digital emitido por uma CA, podem ser resumidas, na ligação da chave publica ao nome que o certificado identifica, evitando a falsificação das chaves, na inclusão do nome da CA, data de expiração e assinatura digital da CA emissora [4].

Para emitir um certificado, uma CA deve respeitar deveres e obrigações descritos em um documento público chamado de Declaração de Práticas de Certificação [19].

Para garantir a validade da Autoridade Certificadora que assinou o certificado, é necessária a definição de uma infra-estrutura técnica e legal, normatizando práticas que suportem as transações eletrônicas com técnicas eficientes no combate aos problemas de segurança do próprio meio.

A solução apresentada é a chamada Infra-estrutura de Chave Pública (ICP ou PKI - *Public Key Infrastructure*) que fornece, através da internet, meios para identificação segura das pessoas e garante a integridade dos registros e sigilo da informação. A PKI associa pessoas a chaves para a criação de uma assinatura digital, visando à realização de negócios eletrônicos eficazes e seguros.

A validade jurídica da certificação digital no Brasil foi regulamentada em 24 de agosto de 2001, pela Medida Provisória 2.200-2, que constituiu a chamada Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil).

As diretrizes propostas na medida têm efeito de lei e desde então não sofreram modificações significativas.

De acordo com o artigo 10, parágrafo 1º desta MP, "os documentos eletrônicos produzidos com a utilização de certificação disponibilizados pela ICP-Brasil" possuem validade jurídica.

A autoridade certificadora raiz da cadeia da ICP-Brasil tem como função básica a execução das políticas de certificados e normas técnicas e operacionais. No Brasil, é representada unicamente pelo Instituto Nacional de Tecnologia da Informação.

Além das vantagens citadas, o uso de certificados deve fornecer uma garantia de sigilo e privacidade, identificação do remetente de uma mensagem, não havendo mais dúvidas sobre a identidade do emissor, e garantia do não-repúdio, fazendo com que um documento eletrônico possua uma validade jurídica, impossibilitando que um usuário afirme que não realizou determinada transação [18].

V. ARQUITETURA DE AUTENTICAÇÃO DE SELOS DE PRIVACIDADE

Reconhecida a importância da regulamentação das atividades relacionadas à coleta de informações dos usuários na Internet, a existência de mecanismos e entidades que garantam segurança das informações dos usuários é justificada, pois a legislação garante a proteção da privacidade, mesmo não havendo lei específica sobre o assunto.

Na existência de invasão da privacidade do usuário, mecanismos podem ser utilizados para evidenciar e provar o abuso. Essas ferramentas policiam as atitudes de sites e garantem segurança de dados do usuário no acesso a serviços da *Web*.

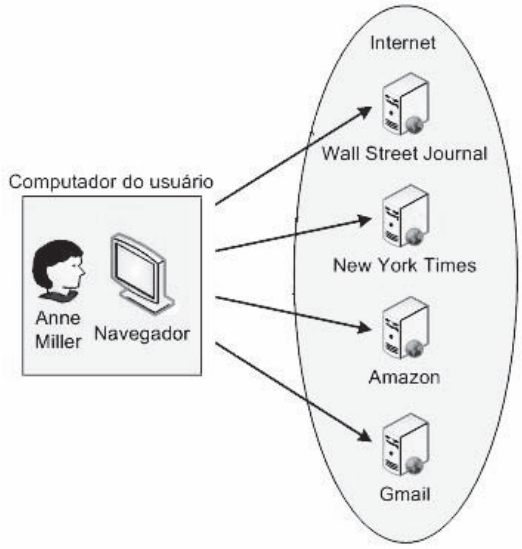


Fig. 1. Usuário acessa diretamente sites da internet

Realizando-se a regulamentação necessária aos serviços relacionados à coleta e manipulação de informações dos usuários, a apresentação de provas materiais será facilitada.

Quando houver a ocorrência de delitos que violem o direito à privacidade do usuário, uma estrutura de autenticação com validade jurídica garante o não-repúdio das ações.

Dessa forma, uma estrutura que permita supervisionar e garantir o comportamento correto de sites na coleta e no manuseio de informações é apresentada. Através das leis existentes, esse mecanismo impõe um regime de boa conduta a empreendimentos on-line.

Num cenário comum, o usuário acessa sites diversos utilizando um navegador da *Web* de forma direta, como demonstrado na Figura 1.

A descrição formal apresentada pela Plataforma 3P é usada para descrever as políticas de privacidade. Um agente do usuário pode analisar estas políticas e informá-lo, garantindo-lhe um poder de escolha sobre o site. A Figura 2 demonstra a navegação com o auxílio de um agente do usuário.

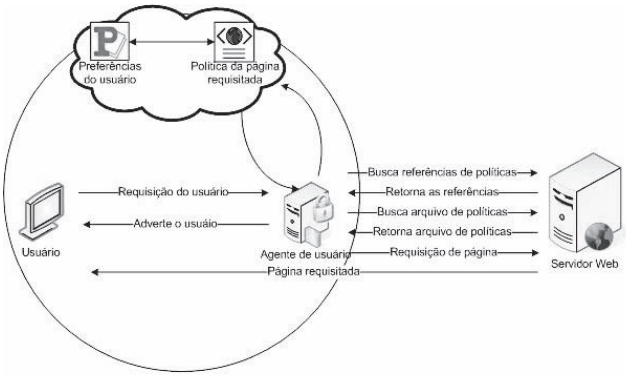


Fig. 2. Acesso com auxílio de agente do usuário para leituras das políticas de privacidade descritas em P3P

Através do uso de selos de privacidade, como demonstrado na Figura 3, a análise feita pelo agente de usuário fica garantida, pois tais selos são fornecidos por uma entidade confiável e conhecida.

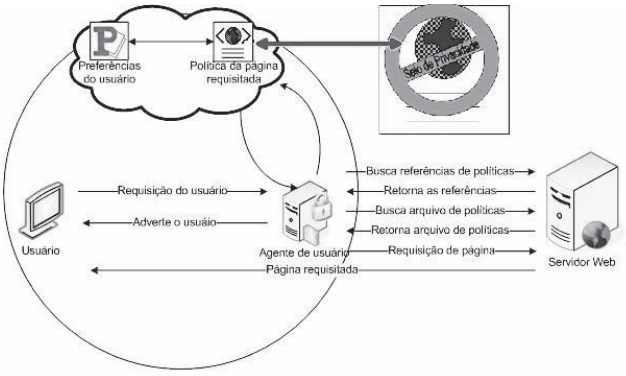


Fig. 3. Utilização de Selo de Privacidade na Política Descrita pelo Site *Web*

A utilização de selos de privacidade garante aos usuários certo nível de confiabilidade nas políticas descritas pelos sites. Políticas estas, que muitas vezes nem são lidas pelos usuários, mas que podem ganhar maior relevância na melhoria de suas declarações e na criação de garantias de privacidade.

As declarações da política devem ser objetivas e estarem escritas em um linguajar apropriado para os visitantes de um site específico. As garantias são providas por entidades confiáveis que supervisionam as atitudes irregulares de coleta e manuseio de informações de usuários da *Web*.

Um problema que ocorre é que os selos não possuem validade legal, para tanto é necessário algo que o valide.

Sendo assim, nessa estrutura de verificação, os certificados digitais são utilizados para delimitar os selos de privacidade.

Como descrito na figura 4, as propriedades da criptografia assimétrica asseguram a confiabilidade e a autenticidade da identidade do site, da entidade que emitiu o selo e do próprio selo. Informações que identificam o site são inseridas nesse novo selo de privacidade. A assinatura da entidade de privacidade, que atua como uma autoridade certificadora, garante a autenticidade do selo.

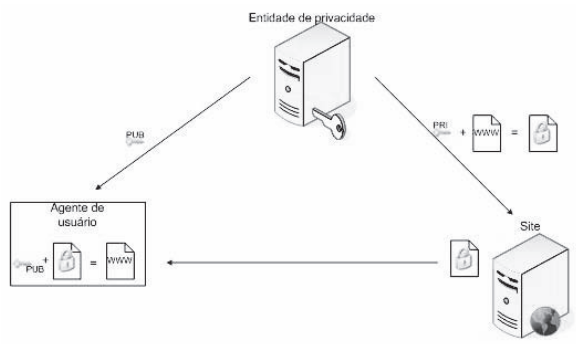


Fig. 4. Processo de Verificação da Autenticidade de um Selo de Privacidade

Essa verificação do selo concedido insere validade jurídica na transação entre o usuário e os sites *Web*. Esse processo de análise de políticas de privacidade e de verificação de uma entidade de privacidade propicia maior confiança ao usuário de que o comportamento dos sites que ele visita é correto.

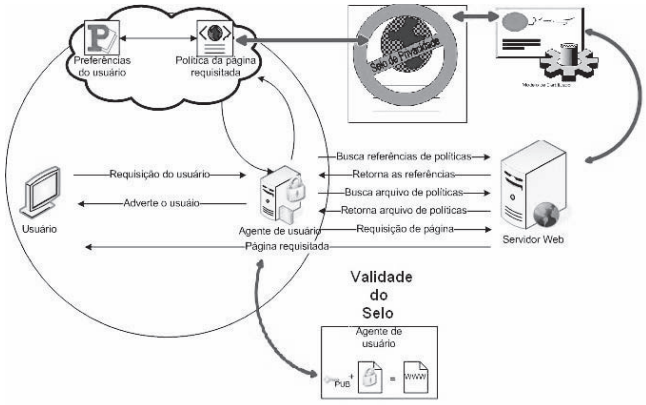


Fig. 5. Visão Geral da Arquitetura

Portanto, a estrutura composta pela verificação automática de políticas de privacidade, pela validação de selos e pela certificação digital, na Figura 5, garante para o usuário segurança de suas informações nas transações no acesso a serviços na *Web*.

VI. CONCLUSÃO

Através do exposto, pode-se verificar que é de suma importância a regulamentação das atividades relacionadas à coleta de informações dos usuários na internet, pois a legislação brasileira garante, de certa forma, a proteção da privacidade, mesmo não havendo lei específica sobre o assunto.

Ressaltando-se que, por proteção entende-se a garantia de reparação de dano – e, algumas vezes, a tipificação penal -, mas não o policiamento para assegurar a privacidade dos usuários.

Mesmo assim, a adequação de leis apenas será efetiva quando houver mudanças em âmbitos sociais, culturais e políticas.

Realizando-se a regulamentação necessária aos serviços

relacionados à coleta e manipulação de informações dos usuários tornar-se-á mais fácil a apresentação de provas materiais, quando houver a ocorrência de delitos que violem o direito à privacidade dos usuários.

A utilização de selos de privacidade garante aos usuários certo nível de confiabilidade nas políticas descritas pelos sites. Políticas estas, que muitas vezes não são lidas pelos mesmos.

Utilizando-se políticas descritas através da Plataforma 3P e validando-as com selos de privacidade de entidades confiáveis, conhecidas e com validade jurídica, traria aos usuários uma melhor sensação de que sua privacidade é respeitada. Garantindo, através do mecanismo de certificação digital, que um selo emitido a um site não seja forjado, também será garantida a identidade do site, da entidade que emitiu tal selo e do próprio selo.

Não há, no Brasil, órgão competente e não é conhecido projeto de lei sobre a criação de órgão regulador no uso de selos de privacidade com validade jurídica.

Assim, a criação de órgão competente para gerenciar as políticas de privacidade, estabelecendo regras de conduta sobre o tratamento da privacidade dos usuários é sugerida.
Esta possível entidade poderia, além de realizar a regulamentação, receber denuncias de usuários sobre violação de privacidade, realizar treinamentos, divulgações com sugestões, cartilhas, etc.

REFERÊNCIAS

[1] M. S. Ackerman e L. F. Cranor, "*Privacy critics safeguarding users personal data*". Web Techniques, Setembro 1999. Disponível em: http://www.webtechniques.com/archives/1999/09/ackerman

[2] G. M. Almeida, *"As Empresas podem "grampear" o e-mail de seus funcionários?"*. Módulo e-Security News. Rio de Janeiro. 1999. Disponível em: http://www.modulo.com.br

[3] M. Bond, D. Haywood, D. Law, A. Longshaw e P. Roxburgh, *"Yourself J2EE in 21 Days"*, I Edição, Pearson Education Inc.

[4] S. Cable, *"Professional Java Web Services"*. Capítulo 6. AltaBooks, 2002.

[5] J. A. Harvey, K. M. Sanzaro, *"P3P and IE 6: Good privacy medicine or mere placebo?"* Computer and Internet Lawyer, 19(4):1–6, April 2002.

[6] H. Hochheiser, *"Principles for privacy protection software"*. Proc. of 10th conf. On Computer, Freedom and Privacy: challenging the assumption, pages 69–72, 2000.

[7] H. Hochheiser, *"The platform for privacy preferences as a social protocol: An examination within the U.S. policy context"*. ACM Transactions on Internet Technology, 2(4):276–306, November 2002.

[8] L. Ishitani, *"Uma Arquitetura para Controle de Privacidade na Web"*. Tese de doutorado: Departamento de Ciência da Computação da Universidade Federal de Minas Gerais, 2003.

[9] A. Kobsa, *"Personalized Hypermedia and International Privacy"*. Communications of the ACM. May, 2002.

[10] B. Mai, N. Menon, S. Sarkar, *"Online Privacy at a Premium"*. XXXVI Hawaii International Conference on Sistems Sciences, 2006.

[11] Mcbride, Baker e Coles. *"E-Commerce Spotlight"*. Summary of ECommerce Legislation. Disponível em: http://www.mbc.com

[12] T. T. Moores e G. Dhillon, *"Do privacy seals in e-commerce really work?"*. Communications of the ACM. December, 2003.

[13] L. M. Paesani, *"Direito e Internet - Liberdade de Informação, Privacidade e Responsabilidade Civil"*. São Paulo: Editora Atlas, 2003.

[14] *"Trust in the wired Americas"*. Cheskin Research (July, 2000). Disponível em: http://www.cheskin.com/think/pressreleases/fprivreport.pdf

[15] G.L. Urban, F. Sultan e W. J. Qualls. *"Placing trust at the center of your Internet strategy"*. MIT Sloan Management Review 42 1 (2000), 39–48.

[16] H. Wang, et al. *"Consumer privacy concerns about internet marketing"*. Communications of the ACM, 41(3): March 1998.

[17] S. Warren e L. D. Brandeis, *"The Right to Privacy"*. HARVARD LAW REVIEW. Vol. 04, fls. 193, 1980. Disponível em: http://www.louisville.edu/library/law/brandeis/privacy.html

[18] *"Certificação Digital – Entenda e Utilize"*. Acessado em 02 de Setembro de 2006. Disponível em: http://www.iti.br/twiki/pub/Main/Cartilhas/CertificacaoDigital.pdf

[19] *"O que é Certificação Digital?"*. Acessado em 02 de Setembro de 2006. Disponível em: http://www.iti.br/twiki/pub/Main/Cartilhas/brochura01.pdf

[20] A. M. Silva Neto, *"E-mails indesejados luz do direito"*. Editora Quartier Latin, 2002.

[21] A. M. Silva Neto, *"O anonimato na Web"*. Disponível em: http://www.advogado.com/internet/zip/anonimo.htm

[22] A. M. Silva Neto, *"Cookies, esses indigestos biscoitos"*. Disponível em: http://www.advogado.com/internet/zip/cookies.htm

[23] C, LUCENA NETO, *"Função social da privacidade"*. Módulo Security, 2002. Disponível em: www.modulo.com.br/pdf/funcaosocialpriv.pdf

[24] C. S. Hall, G. Lindzey, *"Theories of Personality"*. John Wiley & Sons,3rd edition edition, 1978.

[25] *"Constituição Federal do Brasil"*. Disponível em: https://www.planalto.gov.br/ccivil 03/Constituição/Constituicao.htm

[26] *"Código Penal Brasileiro"*. Disponível em: http://www.planalto.gov.br/CCIVIL 03/Decreto-Lei/Del2848.htm

[27] *"Lei de Contravenções Penais no Brasil"*. Disponível em: http://www.planalto.gov.br/Ccivil 03/Decreto-Lei/Del3688.htm

[28] *"Código Civil Brasileiro"*. Disponível em: http://www.planalto.gov.br/CCIVIL/leis/2002/L10406.htm

[29] *"Código de Defesa do Consumidor"*. Disponível em: http://www.planalto.gov.br/ccivil 03/Leis/L8078.htm

[30] *"Lei de Interceptação Telefônica"*. Disponível em: https://www.planalto.gov.br/ccivil 03/LEIS/L9296.htm

[31] *"Projeto de lei 3.360/00 pelo Senador Nelson Proença"*. Disponível em: http://www.camara.gov.br/sileg/Prop Detalhe.asp?id=19533

[32] *"Comitê Gestor da Internet no Brasil"*. Disponível em: http://www.cgi.br

[33] "Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil". Disponível em: http://www.cert.br

[34] *"Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil"*. Disponível em: http://www.cert.br

[35] R. E. Grande, *"Sistema de Integração de Técnicas de Proteção de Privacidade Permitindo Personalização"*. Qualificação de Mestrado: Universidade Federal de São Carlos, 2005.

[36] L. L. Lobatto, S. D. Zorzo, *"Avaliação dos Mecanismos de Privacidade e Personalização na Web"*. In: XXXII Conferencia Latino-americana de Informática CLEI 2006. Santiago, Chile. August, 2006.

Cyber Crimes – a trilha do dinheiro

Pedro Bueno, *McAfee AvertLabs / SANS Internet Storm Center*

There was a time when major crimes committed via the Internet were done mostly by teenage pranksters, and major crimes committed in real life were largely done by adult criminals. Unfortunately these days are gone. Criminal organizations have discovered that online illegal activity can be as profitable as running a real-life scam or an illegal business. Organized crime, mafia groups, and terrorist groups are now using the Internet for illegal fund raising, fraud schemes, and money laundering. This paper will "follow the money" to show how the Internet is being used to finance terrorist groups and support organized criminal activity. We will also demonstrate why Cyber-Terrorism is not only acts of targeting other nation's cyber infrastructure, but also a means to funnel cyber cash to real-life terrorist groups.

I. Introdução

Desde os atentados de 11 de Setembro, os grupos terroristas têm estado sob uma maior vigilância por parte das autoridades. No mundo cibernético não foi diferente, com o aparecimento cada vez maior do chamado cyber terrorismo, e já é possível dizer que os soldados perderam o monopólio da guerra como era conhecida [1]. Apesar da definição de cyber terrorismo caracterizar dano e destruição através do comprometimento de sistemas, neste artigo iremos ver uma outra visão, a de como técnicas de crimes cibernéticos têm sido utilizadas para financiar organizações criminosas, incluindo o terrorismo no mundo real.

II. MOTIVAÇÃO

A. *Financiamento Ilegal*

Como qualquer grupo criminoso, seja o crime organizado ou o terrorismo, as ações precisam ser financiadas, para qualquer que seja o objetivo, como a compra de armamentos, planos estratégicos, operações e treinamento.

B. *Terrorismo*

O terrorismo, devido aos fatos ocorridos nos últimos anos, vem oferecendo uma série de exemplos desta interligação entre o real e o virtual:

1) Em 1999, um hacker com nickname NeOh, foi procurado um grupo do oriente médio para conseguir os planos estruturais de um AirBus A300, com a promessa de receber 10000 USD. Os planos foram conseguidos, mas ele nunca recebeu o prometido. Acredita-se que alguns destes planos foram fundamentais para o seqüestro de um avião da Indian Airlines no Afeganistão em dezembro de 1999. [2]

2) Em fevereiro de 2001, o hacker Ne0h foi novamente abordado pelo mesmo grupo que prometeu o dobro do pagamento por alguns outros planos de aeronaves, mas o hacker, como não havia recebido na primeira vez, desistiu. Descobriu-se que os planos eram para aeronaves idênticas as utilizadas no atentado de 11 de setembro. [2]

3) Acredita-se que o atentado a bombas em uma boate em Bali em 2002 foi parcialmente financiado graças a fraudes online com cartões de crédito. O autor destes atentados, Imam Samudra, possui um livro publicado cujo titulo é "Aku Mekawan Terroris!", cuja tradução para o inglês é "Me Against the Terrorist!", que possui um capitulo chamado "Hacking, why not".[3]

4) Em Abril de 2006, 5 parentes de um jordaniano com cidadania americana acusado de ser um contato da Al Qeada foram presos na Califórnia (EUA) acusados fraudar bancos em centenas de milhares de dólares, com financiamentos e empréstimos. Investigações mostraram que parte do dinheiro foi transferido para uma conta em Amman, na Jordânia. [11]

C. *O modelo Máfia*

Com os altos lucros obtidos com as ações criminosas, um outro modelo real de crime organizado está migrando para o mundo virtual, a Máfia. Um exemplo recente apontado pelo FBI é o CardPlanet [4]. Esse grupo de crime organizado possui a mesma estrutura que a Máfia italiana, e possuía vários outros grupos 'afiliados', como o grupo hacker russo chamado Mazafaka (cujo site web possui o sugestivo titulo "Network Terrorism" [5]), ShadowCrew e IAACA cuja sigla em inglês significa International Association for the Advancement of Criminal Activity.

III . MÉTODOS UTILIZADOS PARA OBTENÇÃO ILEGAL DE RECURSOS FINANCEIROS

A. Roubo de Identidade

O crescimento da internet permitiu que os esquemas tradicionais de fraude tivessem um significativo aumento, graças a utilização e a facilidade que a mesma oferece. Os comprometimentos e invasões de bases de dados de cartões de credito e instituições financeiras para obtenção de informações sensíveis como números de identificação de cartões de crédito fez com que os crimes de roubo de identidade subissem.

O impacto dessas ações é maior que apenas a perda de dinheiro, e é ainda mais grave se pensarmos que terroristas tem utilizado essas técnicas para obtenção de financiamentos e empréstimos. Um exemplo é o de células da Al Qaeda que utilizavam cartões de credito roubados em compras de celulares que eram utilizados para comunicação com outras células terroristas no Paquistão, Afeganistão, Líbano, etc...[6]

B. Phishing (1.0 e 2.0)

1) Phishing 1.0 é o phishing tradicional, que funciona da seguinte maneira:

I. UMA REPLICA DA PAGINA DE UM BANCO É HOSPEDADO EM UM SERVIDOR (PREFERENCIALMENTE UM SERVIDOR DE HOSPEDAGEM GRATUITA).

II. O USUÁRIO RECEBE UM E-MAIL OU DE ALGUMA OUTRA MANEIRA É LEVADO A CLICAR NESTE LINK FALSO, ACHANDO QUE É O LINK DO SEU BANCO.

III. COMO A PÁGINA É UMA RÉPLICA DO SITE DO SEU BANCO, O USUÁRIO IRÁ INSERIR SUAS CREDENCIAIS NESTE SITE, E ASSIM QUE CONFIRMAR ESSES DADOS SERÁ REDIRECIONADO AO WEBSITE VERDADEIRO DE SEU BANCO.

IV. COM BASE NOS DADOS CAPTURADOS O HACKER PODE UTILIZAR PARA REALIZAR TRANSAÇÕES FINANCEIRAS ILEGAIS.

A figura abaixo ilustra o caso típico de Phishing 1.0, com uma página falsa do Banco Santander, hospedada em um servidor no Reino Unido.

Figura 1 – Phishing Santander

2) Phishing 2.0

Com o passar dos anos, as instituições financeiras passaram a implementar novas técnicas de segurança para seus clientes. O Phishing 2.0[12], a segunda geração dos phishings, tem como objetivo principal tentar *bypassar* essas novas proteções, como:

I. - OTP – one time password. Um exemplo desse tipo de proteção são os Token que geram novos números a cada 30/60 segundos, sendo esta a senha da pessoa.

II. - IP Geolocation – o banco associa a conta da pessoal com a localidade dela, assim uma pessoal na Rússia não pode acessar a conta de um banco brasileiro.

O Phishing 2.0 funciona da seguinte maneira:

1. O usuário é levado a clicar em um link de seu banco
2. O site com o phishing na verdade não é um site com uma replica do site do seu banco, mas um servidor proxy que conecta ao site real do banco.
3. O hacker toma conta da sessão assim que o usuário se 'loga' no banco
4. Quando o usuário sai, o proxy continua ativo, fazendo 'refreshes' para evitar um timeout
5. O hacker pode alterar a sessão de acordo com suas necessidades.

Um exemplo:
- O cliente fala para o proxy: Transfira 1000 reais para conta XXX / Ag YYY
- O proxy fala para o banco: Transfira 1000 reais para conta AAA / Ag BBB
- O banco para o proxy: Confirma transferência de 1000 reais para conta AAA / Ag BBB
- O proxy fala para o cliente: Confirma transferência de 1000 reais para conta XXX / Ag YYY
- O cliente fala para o Proxy: Confirmo transferência para XXX / YYY e o numero do meu token é 123456
- O proxy fala para o banco: Confirmo transferência para AAA / BBB e o numero do meu token é 123456.

Figura 2 – Funcionamento do Phishing 2.0

Para *bypassar* a proteção do IP Geolocation, o Phishing 2.0 utiliza uma botnet para escolher um proxy que esteja em uma

região do banco.

3) *Bankers 1.0*

Os trojans bancários, também chamados de Pws-Banker são malwares cujo objetivo é o de se instalar na máquina da pessoa e monitorar seu trafego. Quando o usuário for entrar em uma pagina do seu banco, o trojan irá carregar uma aplicação que irá simular a pagina do seu banco e capturar as informações do cliente. Normalmente esses trojans são constituídos de 2 componentes:

I. DOWNLOADER – os downloaders normalmente são baixados ao clicar em links de e-mails falsos, como Cartões Virtuais, Orkut, Comunicados (SERASA, SPC, TSE).

É importante notar que muitas vezes os e-mails são criados e distribuídos com tanta pressa e sem "controle de qualidade", que as vezes é possível ver um e-mail cujo remetente é "Americanas.com" e o assunto "Justiça Eleitoral".

Ao clicar nesses links para baixar um "formulário", "cartão", etc... o downloader irá fazer, em background, o download do componente principal, o Pws-Banker.

A razão de se ter 2 componentes é que o downloader tem em média 10 a 20kb de tamanho, ou seja, extremamente rápido de ser baixado, enquanto o Pws-Banker pode variar de 500kb a 2Mb, o que seria muito lento e poderia levantar suspeitas do usuário.

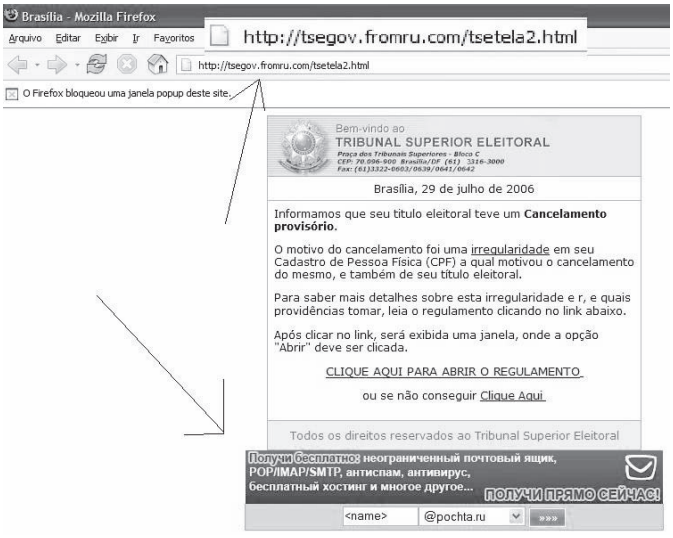


Figura 3 - Exemplo de Phishing para Downloader

A figura acima mostra um exemplo real de um falso aviso do Tribunal Superior Eleitoral, hospedado em um site na Russia, que inclusive contem banners em russo.

II. Pws-Banker – o pws-banker é o software que irá monitorar as urls dos principais bancos e simular a pagina do banco quando o usuário tentar acessá-la. Assim que obtiver as informações, ele envia um email para o hacker, para que o mesmo possa acessar o banco com as credenciais do cliente, e assim poder realizar transferências ilegais.

As informações são transmitidas no seguinte formato:

```
>>B.a.c.o.d.o=B.r.a.s.i.l<<<
=-=-=-=CAIXA ECONOMICA FEDERAL=-=-=-=
=-=-=-=BANCO REAL=-=-=-=
=-=-=-=UNIBANCO=-=-=-=
![Titu].....:
![Age].....:
![Cont].....:
![SeAA].....:
![SeCart]....:
=-=Tabela=-=
=-=Chave20:
=-=Chave25:
=-=Chave33:
=-=Chave35:
=-=Chave11:
=-=Chave17:
=-=Chave52:
```

Figura 4 – Exemplo dos dados transmitidos

4) *Bankers 2.0*

A segunda geração dos Bankers, chamada de Bankers 2.0[8] apresenta duas modificações em relação a sua versão anterior:

I. Targeted Bank – o contrario do antigo trojan bancário que tinha a capacidade de simular paginas de vários bancos diferentes, o novo Pws-banker é direcionado a algum banco especifico que tenha um método de proteção especifico. Um exemplo é o PWS-Banker.gen.t[9], que era direcionado ao Banco Bradesco, e que realizava um harvesting no HD do cliente, em busca de arquivos do tipo *.crt e *.key, utilizados para certificação digital, um outro método de prover maior segurança ao acesso a internet banking.

II. Modular – a segunda modificação é que a arquitetura desses trojans agora é modular. Ou seja:

a) Usuário é levado a baixar o downloader
b) Downloader busca o arquivo links.jpg do site www.free.ru (na Rússia)
c) Arquivo links.jpg na verdade é um arquivo texto que contem links para o downloader baixar arquivos específicos do site www.free.cn (na China).

d) Downloader baixa do site www.free.cn, pws-bankers direcionados para alguns bancos específicos.

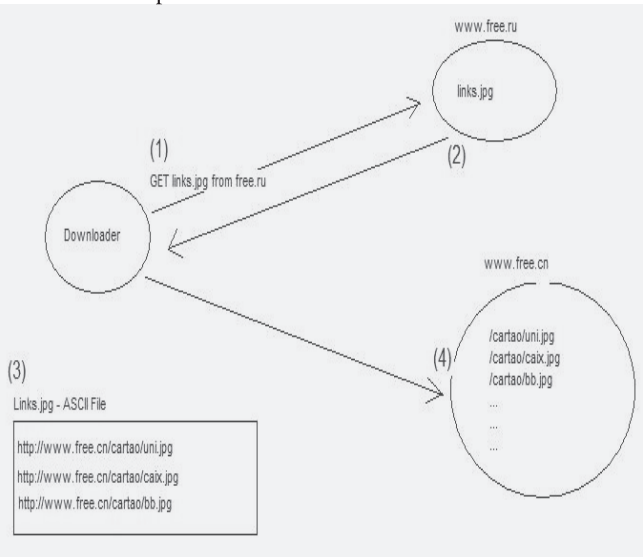


Figura 5 – Fucionamento do Banker 2.0

Neste exemplo, a escolha dos domínios .ru e .cn não foram aleatórias. A escolha dos lugares para hospedagem dos trojans geralmente também não é aleatória, pois a intenção é manter esses trojans disponíveis pelo maior tempo possível. E a ação de remoção de trojans em sites de hospedagens (gratuitas ou não) nestes paises é extremamente complicada devido a barreira da língua, ficando assim um maior tempo disponível.

5) Botnets

- Uma outra forma de obter ganhos financeiros é através da utilização das botnets. Em resumo, uma botnet é o conjunto de bots, que caracterizam um computador sob o domínio remoto de um hacker (máquinas zombies).

As botnets podem variar de tamanho, com poucas máquinas à até milhões de maquinas[10]. Elas já tem sido utilizadas a alguns anos para os mais variados propósitos, como:

A. Armazenamento de conteúdo copyrighted – esses conteúdos podem variar de sofwares, livros e videos piratas

B. Envio de spams – esses spams podem conter links para phishings e downloads de Pws-bankers

C. Ataques DDoS – esses ataques podem servir como duas fontes diferentes de ganhos financeiros:

✓ Venda de ataques a algum site de competidor.

Em 2004, Saad Echouafni, CEO da empresa Orbit Telecomunications, foi condenado por contratar um ataque de DDoS a sites de competidores, provocando perdas de cerca de 1 milhão de dólares.

✓ Extorsão de um site, no qual ele paga uma quantia para ter a 'proteção' que não irá receber um ataque de DDoS e ficar indisponível e perder milhares de dólares pelo tempo do ataque, no qual os clientes não terão acesso ao site.

Em outubro de 2005, uma botnet com mais de 1.5 milhões de máquinas foi descoberta na Holanda, e a prisão de 3 homens indicava que os mesmos trabalhavam para o crime organizado russo, chamada "Russian Internet Máfia".

IV CONCLUSÃO

A utilização da internet pelos grupos que promovem atividades ilegais, como grupos extremistas armados, Máfia e crime organizado é cada vez mais perceptível, assim como a interação entre os mesmos e os métodos utilizados. Com tamanha interação e a clara motivação financeira entre estes grupos, fica claro como o contra-ataque das autoridades está um passo atrás. Um possível caminho para se chegar ao estagio atual dos criminosos é o compartilhamento de informações entre a comunidade de segurança de informações e as autoridades responsáveis por combater os mesmos. Fabricantes de Anti-Virus, IDSs, Listas de segurança fechadas são apenas alguns exemplos por onde esse fluxo de informações poderia passar.

Finalmente, o importante a ser notado é que se atitudes como essa não foram tomadas, estaremos sempre fadados a estarmos em modo reativo, ao invés de estamos tomando ações pró-ativas visando a proteção do usuário final.

REFERENCIAS

[1] Liang Quiao. 1999. Unrestricted Warfare
[2] Sachs, Marcus. et all. 2004 Cyber Adversary Characterization – Auditing the hacker mind. Syngress
[3] Emerging Terrorist Capabilities for Cyber Conflict against the U.S. Homeland. Disponível em http://www.cyberconflict.org/pdf/WilsonNov012005.pdf
[4] FBI: Cybercriminals taking cues fromMafia –Disponíveç em http://www.infoworld.com/article/06/08/07/HNcybercriminals_1.html
[5] Mazafaka Network Terrorism Group. Disponível em http://www1.mazafaka.ru/
[6] FBI Congressional Testimony. Disponível em http://www.fbi.gov/congress/congress02/idtheft.htm
[7] Botnets – f-secure blog
[8] Bankers 2.0. Disponível em http://isc.sans.org/diary.php?storyid=1543
[9] McAfee Vil Description. Disponível em: http://vil.nai.com/vil/content/v_140334.htm
[10] Dutch Botnet Trio Reportedly Connected to Russian Mob. Disponível em http://www.techweb.com/wire/security/173600331
[11] Five Relatives of Terrorism suspect arrested. Disponível em: http://www.msnbc.msn.com/id/12523560/from/RSS/
[12] Phishing 2.0 - http://biz.yahoo.com/prnews/060712/sfw062.html?.v=67

Pedro Bueno was the coordinator of the CSIRT at one of the Brazil's largest Telecom companies and is currently a Anti-Virus Research Engineer at McAfee AvertLabs. He is one of the handlers at the SANS Institute's Internet Storm Center, where he deals daily with cutting edge security issues and authored a series of the Malware Analysis Quizes. He is also a member of The SANS Top 20 Internet Security Vulnerabilities expert's Team for about 5 years.

Detecting Attacks in Electric Power System Critical Infrastructure Using Rough Classification Algorithm

Maurĭio Pereira Coutinho, Germano Lambert-Torres, *Member,* IEEE,
Luiz Eduardo Borges da Silva, *Member,* IEEE, and Horst Lazarek

***Abstract*— This paper presented an alternative technique to improve the security of Electric Power Control Systems by using anomaly detection to identify attacks and faults. By using Rough Sets Classification Algorithm, a set of rules can be defined. The alternative approach tries to reduce the number of input variables and the number of examples, offering a more compact set of examples in order to fix the rules to the anomaly detection process. An illustrative example is presented.**

***Index Terms*—Electric power system, detecting attacks, rough set theory, data mining.**

I. Introduction to Critical Infrastructures

NOWADAYS, Critical Infrastructure plays a fundamental role in our modern society. Telecommunication and transportation services, water and electricity supply, and banking and financial services are examples of such infrastructures that provide critical services to our communities. The interconnection of such structures and the use of information technology in order to achieve quality of their services expose the society to more vulnerabilities and security threats. With a computer and an Internet connection, intruders can remotely access interconnected and interdependent Critical Infrastructures to interrupt important services. To safeguard against the threat of such cyber-attacks, providers of Critical Infrastructure services also need to maintain the accuracy, assurance and integrity of their interdependent data networks.

In United States of America, Critical Infrastructures are defined according the USA Patriot Act of 2001 as "*systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national health or safety, or any combination of those matters*". The following Critical Infrastructure Sectors are identified in [1]: *Agriculture and Food, Banking and Finance, Chemicals and Hazardous Materials, Defence Industrial Base, Emergency Services, Energy, Higher Education, Insurance, Law Enforcement, Oil and Gas, Postal and Shipping, Public Health, Telecommunications and Information Technology, Transportation, Water, Commercial Key Assets, Dams, Governments Facilities, National Monuments and Icons, Nuclear Power Plants*. Accordingly to [2], a Critical Infrastructure can be divided into the following three layers: physical layer, cyber layer, and human operations layer. In the past, physical and human operations layers have been more vulnerable to attacks. Nowadays, we are seen the increase in the vulnerability of the cyber layer.

Manuscript received September 24, 2006. This work was supported in part by the Brazilian Research Council (CNPq) and Minas Gerais State Research Foundation (FAPEMIG).

M. P. Coutinho, G. Lambert-Torres, and L.E. Borges da Silva are with the Federal University of Itajuba (UNIFEI), Itajuba, MG, 37500-503, Brazil (phone: +55-35-36291240; fax: +55-35-3629118755; e-mail: {coutinho, germanoltorres}@gmail.com).

H. Lazarek is with the Technical University of Dresden, Dresden, Germany.

II. Initiatives for Security of Critical Infrastructure

Guidance documents, standards, legislations, and regulations in order to improve security of Critical Infrastructures are currently in development around many countries. The initiatives differ with respect to the involved parties and their goals, as well as geographic and industry scope [3]. This section presents some of those initiatives.

Since September, 11, 2001 terrorism and homeland security have taken top priority in U.S. governmental policy and affairs. Examples can be found in the release of "The National Strategy to Secure Cyberspace" [4] and with the official creation of the Department of Homeland Security (DHS) [5]. An initiative of the Eidgenössische Technische Hochschule Zürich (ETHZ) and other partners is "The International Critical Information Infrastructure Protection (CIIP) Handbook" [3] that surveys critical information infrastructure protection efforts in fourteen countries. The main focus is on the national governmental efforts to protect critical information infrastructures. The IT Baseline Protection Manual is a German initiative of the Bundesamt für Sicherheit in der Informationstechnik (BSI) and it recommends a series of standard security measures for typical IT applications and IT systems [6]. In the area of evaluating computer systems and software from a security perspective there are the Trusted Computer System Evaluation Criteria (TCSEC), or the Orange

book, the Information Technology Security Evaluation Criteria (ITSEC), the Common Criteria for Information Technology Security Evaluation (CCITSE)] or ISO/IEC 15408. Another initiative is the "Process Control Security Requirements Forum (PCSRF)", which is a industry group working with security professionals to assess vulnerabilities and establish appropriate strategies for the development of policies to reduce IT security risk within the US process control industry [7]. The ISA Committee SP99 "Manufacturing and Control Systems Security" intends to create guidance documents and a Standard (S99) on introducing IT security to existing industrial control and automation systems [8]. The objective for this IEC standard is to describe state-of-art secure realization of certain common automation networking scenarios [9]. The British Columbia Institute of Technology (BCIT) maintains an Industrial Cyber Security Incident Database, designed to track incidents of a cyber security nature that affect industrial control systems and processes [10].

III. Security Fundamentals

The security objectives offer a framework for categorizing and comparing the security mechanisms of various systems. They are: Confidentiality, Integrity, Availability, Authentication, Authorization, Auditability, Nonrepudiability, and Third-Party Protection. An intentional violation of a security objective is called attack. Attacks may either be initiated by persons outside or by insiders. Some common types of attacks are the following: Denial of Service, Eavesdropping, Spoofing, Man-in-the-Middle, Breaking into system, Virus, Trojan, and Worm [11]. Naedele and Dzung [12] enumerate a relationship between the security objective and the security mechanism.

In [13], it is showed how the increasing sophistication of attacks from the mid-1980s to the present have grown in complexity and in automation in despite of the skill required to launch the attacks has been reduced. This is an indication that this automation may be the trigger for large-scale activity on the internet.

IV. Electric Energy Critical Infrastructure

The Electric Utility Information Technology Systems can be divide in four kinds: Business Computers, Engineering Computers, Control Centre Computers, and Embedded Computers [14]. The use of Information Technology in the Control Centre Computers and Embedded Computers started, approximately, 3 decades ago. The operational structure used for this is based on data validation/conformation process to the supervisory and control system. This process is realized in 3 steps: Data Acquisition, Data Conditioning and Data Conversion. After this the data is inserted into the control and/or supervisory computer, where the specific treatment is accomplished and the actions are taken in order to maintain the behaviour and reliability of the system. See Fig. 1.

In general, a Electricity Cyber Infrastructure is highly interconnected and dynamic, consisting in several utilities. Due to its hierarchical organization, it is sub-divided into regional grids. Each sector is further split into generation, transmission, distribution and customer service systems, supplemented with an energy trading system. The Power Grid is comprised of a myriad of assets, such as Generation Plants, Transmission Lines, Transmission and Distribution Power Substations, Local, Regional and National Control Centres, Remote Terminal Units (RTUs)/Intelligent Electronic Devices (IEDs), and Communication Links [15].

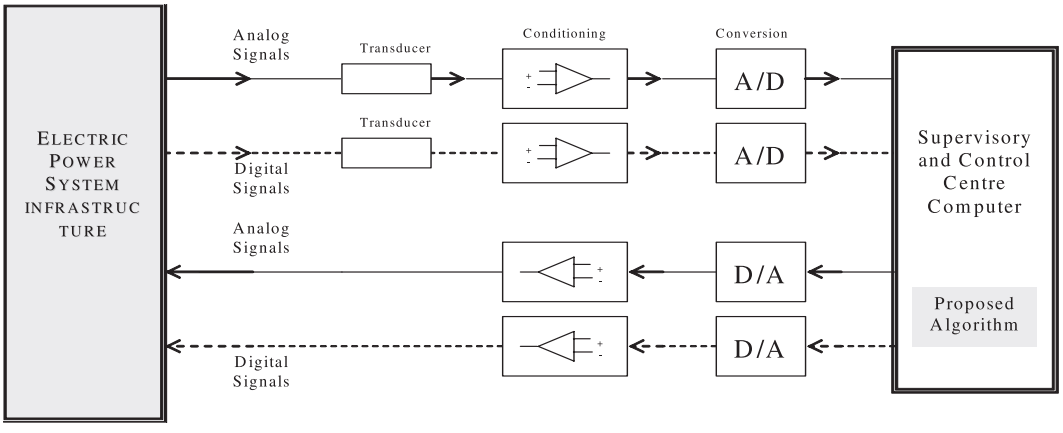


Fig. 1. Basic Block Diagram for a Digital Control System

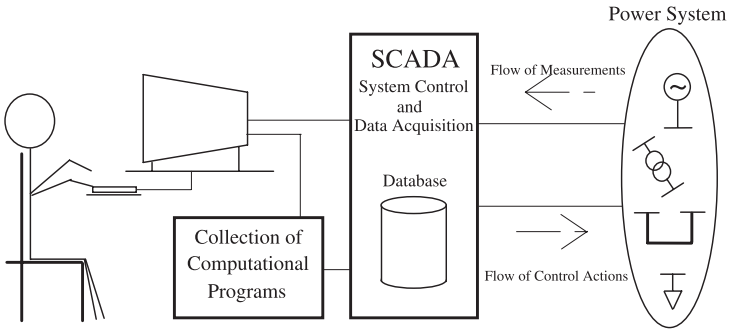


Fig. 2) Electricity cyber infrastructure.

The computer electricity cyber infrastructure can be divided in 2 parts: Electric Management Systems, which allow operators to regulate power flow, and the Supervisory Control and Data Acquisition (SCADA) systems for monitoring the safety, reliability, and protective functions of the power grid [15]. See Fig. 2.

V. Vulnerabilities in Electric Power Systems

Nowadays SCADA systems are an important part of the nation's Critical Infrastructure. They require protection from a variety of threats and their network are potentially vulnerable to cyber attacks because the proprietary protocols and networks have long been considered immune to attacks and security has not been part their design. The diversity and lack of interoperability in these communication protocols create obstacles for anyone attempting to establish a secure communication. The variety of communications media used to establish the communication links contributes for increasing of the infrastructure vulnerability [16].

VI. Detecting Attacks

Attacks on computer and network systems have significantly increased in recent years [12]. An intrusion Detection System (IDS) is a "burglar alarm" and has been widely studied in recent years, as in [17-20]. An extended bibliography can be found in [21]. IDSs can be characterized by different monitoring and analysis approaches. They can monitor events at three different levels: network, host, and application. These events can be analysed using two techniques: signature detection and anomaly detection. Anomaly-based IDSs find attacks by identifying unusual behaviour (anomalies) on a host or network. They function on the observation that some attackers behave differently than "normal" users and thus can be detected by systems that identify these differences. The measures and techniques used in anomaly detection include: Threshold detection, Statistical measures, and Rule-based measures [19]. Examples of anomaly detection techniques are IDES [22] and EMERALD [23].

VII. Previous Work

Different approaches have been used in the area of detecting intrusions in computer systems over the past 20 years. Most previous work on anomaly intrusion detection has determined profiles for user behaviour. Intrusions are detected when a user behaves out of character. These anomalies are detected by using statistical profiles, as in IDES [22], inductive pattern generation or neural networks as in [24, 35]. Manikopoulos and Papavassiliou [26] used statistical models using metrics derived from observation of the user's actions. Fink et al [27] focused on determining normal behaviour for privileged process, those that run as root. Another approach took from [24] it is similar to the later but it differs in that they use a much simpler representation of normal behaviour. Anomaly detection schemes also use data mining techniques such as clustering, support vector machines (SVM), and different neural network models. For example, Mukamala [28] describes approaches to intrusion detection using neural networks and SVM. Sekar et al [29] presented an approach that combines specification-based and anomaly-based intrusion detection, mitigating the weaknesses of the two approaches while magnifying their strengths. In [30], a novel multilevel hierarchical Kohonenen Net (K-Map) is introduced. Each level of the Hierarchical Map is modelled as a simple winner-take-all K-Map. The objective was to detect as many different types of attacks as possible. In [31], it is presented a data mining algorithm based on supervised clustering to learn patterns and use these patterns for data classification. In [32], it is presented research results on the detection of network security attacks in computer and control systems through the identification and monitoring of a synthetic "DNA Sequence". Just as DNA characterizes the make up of the human body a "DNA Sequence" of a computer system has similar functions. Changes in behavioural patterns of a computer system, such as virus attacks, are reflected in changes in the DNA Sequence and appropriate actions can be taken. Martinelli et al [33] proposed an approach to monitor and protect Electric Power System by learning normal system behaviour at substations level, and raising an alarm signal when an abnormal status is detected; the problem is addressed by the use of auto-associative neural networks, reading substation measures.

Wang et Battiti [34] proposed a real time network based intrusion identification model based on Principal Component Analysis (PCA). The PCA technique is used to profile normal program and user behaviours for host-based anomaly intrusion detection. Song et al [35] introduces the Hierarchical Random Subset Selection-Dynamic Subset Selection (RSS-DSS) algorithm for dynamically filtering large data sets based on the concepts of training pattern age and difficult, while utilizing a data structure to facilitate the efficient use of memory hierarchies. In [36], it is showed how the accuracy and security of SCADA Systems can be improved by using anomaly detection to identify bad values caused by attacks and faults. The performance of invariant induction and n-gram anomaly-detectors is compared.

VIII. Problem Definition

The operation of a power system is intrinsically complex due to the high degree of uncertainty and the large number of variables involved. The various supervision and control actions require the presence of an operator, who must be capable of efficiently responding to the most diverse requests, by handling various types of data and information.

These data and information come from measurements of SCADA systems or from computational processes. The size of the current database in a power control center has increased a lot in the last years due to the use of network communications. This makes their control systems more vulnerable to manipulation by malicious intruders. In order to improve the security of SCADA systems, anomaly detection can be used to identify corrupted values caused by malicious attacks and faults.

The aim of this paper is to present an alternative technique for implementing anomaly detection to monitor Power Electric Systems. The problem is addressed here by the use of Rough Sets Classification Algorithm, proposed by Pawlak in [37]. Related work can be found in [2, 33, 36, 38, 39].

The system operator needs to know the current state of the system and some forecasted position, such as load forecasting, maintenance scheduling, and so on in order to take a control action (switching, changing taps and voltage levels, and so on). One of the most important operator tasks is to determine the current operational state of the system. To accomplish this task, the operator receives many data from/into the system. By handling these data, the operator tries to build an image of the operation point. Fig.3 shows a representation of this process.

The analysis tries to make an assessment of the operational mode in one of the 2 states: normal, or abnormal. In the first state, normal, all loads are supplied and all measurements are inside of the nominal rates. In the second state, abnormal, all loads continue to be supplied but some of the measurements are outside the nominal rates or some loads are not supplied, i.e., there was a load shedding process.

Even when the operation state is normal, the operator needs to analyze the system security. This analysis is made according to possible contingencies that could affect the power system. Loss of a transmission line, shut down of a power plant or an increase of the load are some contingencies that can occur during the operation. An example of normal or abnormal points is shown in Fig. 3. It shows the same contingency for two different operation points. For the operation point A, the contingency produces an abnormal operation point; while for the operation point B, the system continues in the normal state. Thus, the point A is an unsafe operation point and point B is a safe one.

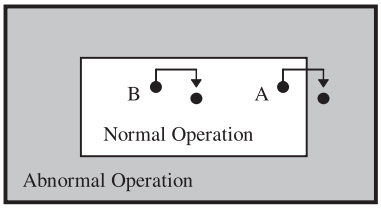


Fig. 3. Operational State of a Power System and Changing of Operation Point

The illustrative example that follows has an objective to describe the fundamentals concepts of the rough set theory applied to anomaly detection. The idea is to transform a set of examples in a set of rules that identify possible intruders. For sake of explanation, some assumptions and reductions are made. This approach gives the opportunity to detail each step of the formulation without reducing generalization.

IX. Description of the Problem

The main purpose of the illustrative example that follows is to help the understanding of the rough set theory fundamental concepts. The idea is to transform a set of examples in a set of rules that represent the operational state of a power system. Some assumptions and simplifications are made to allow a better understanding of each step of the formulation without loss of generality. In fact, the data used in this paper comes from a Brazilian electricity utility.

Consider a control center database composed by a set of measurements, such as the one shown in Table I. The operational state of the hypothetical power system depends on four elements: status of circuit-breaker A, transmission capacity of lines B and C, and voltage of bus D. Moreover, Table 1 contains the attributes represented by the set {A, B, C, D} and the corresponding decision S, where:

- the status of circuit-breaker A is defined by 0 (close) or 1 (open);
- the values of transmission lines B and C are percentages of real power flows according to their maximum capacities, in [%]; and,
- the bus voltage D is expressed as a fraction of the rated voltage.

The classification of each state is made according to an expert (usually, a senior operator/engineer), and four possible outputs can be selected for the power system operational state:

Normal or safe (S) or abnormal or unsafe levels 1,2 and 3 (L1, L2, L3, respectively). These levels can represent malicious actions in SCADA systems performed by the attackers like changing data values, changing information control, opening breakers, fraud, and overload.

TABLE I
REDUCED CONTROL CENTER DATABASE

	Attributes				
U	**A**	**B**	**C**	**D**	**S**
1	0	57	82	1,07	L2
2	0	37	32	0,97	L1
3	1	0	87	0,95	L3
4	1	72	31	1,07	L3
5	0	28	39	1,02	L1
6	0	42	82	1,07	L2
7	0	52	59	1,01	S
8	1	62	67	1,04	L3
9	0	57	45	0,99	S
10	0	45	58	1,00	S
11	0	32	57	0,94	S
12	0	0	57	1,08	L2
13	1	58	87	1,03	L3
14	0	58	56	1,07	L2
15	0	25	57	1,03	S
16	0	56	54	1,08	L2
17	1	59	72	1,08	L3
18	0	32	0	0,93	L1
19	0	32	45	0,94	S
20	1	72	67	0,96	L3
21	0	57	45	1,01	S
22	0	32	45	0,94	S
23	0	29	43	1,08	L2
24	1	0	72	0,95	L3
25	1	57	79	1,07	L3
26	0	31	43	0,99	S
27	0	32	42	0,94	S
28	0	17	32	0,92	L1
29	0	23	22	1,00	L1
30	0	23	57	0,91	S

Observing the above set of examples, it is really hard to conclude that the condition of transmission line B is not necessary in the classification process. Notice that, this attribute is a dispensable one, as shown later. Even in this very small database it is very hard to reach a conclusion. For real control center database, usually with hundreds important attributes and thousands of examples, it could be impossible to take a reliable control action.

X. PRESENTATION OF THE ALGORITHM

Before the presentation of the algorithm, two major concepts in Rough Set theory, *reduct* and *core*, will be defined. These concepts are important in the knowledge base reduction.

Let **R** be a family of equivalence relations. The reduct of **R**, *RED*(**R**), is defined as a reduced set of relations which conserve the same inductive classification of set **R**. The core of **R**, *CORE*(**R**), is the set of relations which appear in all reduct of **R**, i.e., the set of all indispensable relations to characterize the relation **R**. The main idea behind the knowledge base reduction is a simplification of a set of examples. This can be obtained by the following procedure:
a) calculate the core of the problem;
b) eliminate or substitute a variable by another one; and
c) redefine the problem using new basic categories.

The algorithm that provides the reduction of conditions can be represented by the following steps:
Step 1: Redefine the value of each attribute according to a certain metric. In this illustrative example, typical ranges in power system operation are used:

- real power values: under 40% of nominal capacity = low (L), between 40% and 60% = medium (M), and above 60 % of nominal capacity = high (H)
- bus voltage values: under 0.95 pu = low (L), between 0.95 and 1.05 = normal (N), and above 1.05 = high (H)
- the status of circuit-breakers are maintained because the values 0 and 1 are normalized already.

Step 2: This next step verifies if any attribute can be eliminated by repetition.
Step 3: This step verifies and eliminates identical examples.
Step 4: This step verifies if the decision table contains only indispensable attributes. This task can be accomplished eliminating step-by-step each attribute and verifying if the table still gives the correct classification. In the example, after considering the elimination of each attribute, B is dispensable for the decision table.

TABLE II
REDUCTION OF THE SET OF EXAMPLES

	Attributes			
U	**A**	**C**	**D**	**S**
1A	0	-	H	L2
1B	-	M	H	L2
2A	1	H	-	L3
2B	1	-	N	L3
2C	-	H	N	L3
3	-	M	L	S
4	-	L	-	L1
5	-	M	N	S
6A	0	H	-	L2
6B	0	-	H	L2
7	1	-	-	L3
8	-	L	-	L1

Step 5: Compute the core of the set of examples. This can be done eliminating each attribute step-by-step, and verifying if the decision table continues to give the correct answer (i.e., it continues to be consistent).

Step 6: This step computes the reduced set of relations that conserve the same inductive classification of the original set of examples. Table 2 contains the reduction of each example.
Step 7: According to Table II, the knowledge existent in Table I can be expressed by the following set of rules:

- If (C is M and D is L) or (C is M and D is N) then S = Safe.
- If C is L then S = Abnormal level 1.
- If (A is 0 and D is H) or (C is M and D is H) or (A is 0 and C is H) then S = Abnormal level 2.
- If (A is 1) or (C is H and D is N) then S = Abnormal level 3.

or, using a *complete rule formulation*:

If (the power flow in transmission line C is between 40% and 60%) and (the voltage on bus D is below 1.05)
then the classification of the current state of the system is safe.

If the power flow in transmission line C is below 40%
then the classification of the current state of the system is unsafe level 1.

If (the voltage on bus D is above 1.05) and (the circuit-breaker A is closed or the power flow in transmission line C is between 40% and 60%)
then the classification of the current state of the system is unsafe level 2.

If (the power flow in transmission line C is above 60%) and (the circuit-breaker A is closed)
then the classification of the current state of the system is unsafe level 2.

If (the circuit-breaker A is opened)
then the classification of the current state of the system is unsafe level 3.

If (the power flow in transmission line C is above 60%) and (the voltage on bus D is between 0.95 and 1.05)
then the classification of the current state of the system is unsafe level 3.

XI. Conclusions

Critical Infrastructures, such Electric Power Systems, are vital for our modern society. Therefore they require protection from a variety of threats and their network is potentially vulnerable to cyber attacks. Intrusion Detection Systems is an important tool to increase the security of such Critical Infrastructures. This paper presents a systematic approach to transform examples in a reduced set of rules for an anomaly detection. This approach uses Rough Set theory and concepts of core and reduction of knowledge. An example for power system control centers has been developed. For the sake of clarity, a reduced database is used in the illustrative example. However, the same methodology is applicable to larger databases. The illustrative example showed that the technique has many advantages, such as simplicity to implementation and good performance.

References

[1] "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets",Washington D.C.,Feb 2003, http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf

[2] Gamez, D., Nadjm-Tehrani, S., Bigham, J., Balducelli, C., Burbeck, K., and Chyssler, T., "Chapter 19 Safeguarding Critical Infrastructures", Edited by Professor Hassan B. Diab & Professor Albert Y. Zomaya, "Dependable Computing Systems: Paradigms, Performance Issues, and Applications", Wiley STM, 2000.

[3] Dunn, M., and Wigert, I., "International CIIP Handbook 2004", ETHZ, Zurich, 2004.

[4] "The National Strategy to Secure Cyberspace", Washington D.C.,February,2003,http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf.

[5] "Homeland Security Act of 2002", Washington D.C., January, 2002, http://www.dhs.gov/interweb/assetlibrary/hr_5005_enr.pdf.

[6] IT-Grundschutz Manual 2004, http://www.bsi.bund.de/english/gshb/index.htm.

[7] Falco, J., Stouffer, K., Wavering, A., and Proctor, F., "IT Security for Industrial Control Systems", NISTIR 6859, February 2002.

[8] Oyen, R., "Making Sense of the Myriad of Manufacturing and Control System Security Standards, ISA Expo 2005, Oct., 2005.

[9] Naedele, M., "Standardizing Industrial IT Security – A first Look at the IEC Approach", Emerging Technologies and Factory Automation, 2005, ETFA 2005. 10th IEEE Conference on, Vol. 2, 19-22, Sept. 2005, pp. 857 – 863.

[10] Byres, E. and Lowe, J., "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems", VDE 2004 Congress, VDE, Berlin, October, 2004.

[11] Dzung, D., Naedele, M., Von Hoff, T.P., and Crevatin, M., "Security for Industrial Communications Systems", Proceedings of the IEEE, Vol.93, No. 6, June 2005.

[12] Naedele, M., and Dzung, D., "Industrial Information System Security – Part I, Part2, and Part 3", ABB Review 2005.

[13] McHugh, J., Christie, A., and Allen, J., "The role of Intrusion Detection Systems", IEEE Software, September/October/2000.

[14] Hale, J., and Bose, A.,"Information Survivability in the Electric Utility Industry", ISW´98, http://www.cert.org/research/isw/isw98/all_the_papers/no19.html.

[15] Goetz, E., "Cyber Security of the Electric Power Industry", Institute for Security Technology Studies at Dartmouth College", December, 2002 [NERC-CIP,2005] http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection.

[16] Oman, P., Schweitzer, E., and Roberts, J., "Protecting the Grid From Cyber Attack, Part II: Safeguarding IEDS, Substations and SCADA Systems", Utility Automation, 7(1), 2002, pp. 25-32.

[17] Axelsson, S., "Intrusion Detection Systems: A Survey and Taxonomy", Chalmers University of Technology, Göteborg, Sweden, March/2000.

[18] McHugh, J., "Intrusion and Intrusion Detection", International Journal of Information Security, Volume 1, Issue 1, Aug 2001, Pages 14 - 35, DOI 10.1007/s102070100001, URL http://dx.doi.org/10.1007/s102070100001.

[19] Bace, R., and Mell, P. "Intrusion Detection Systems", NIST Special Publication on Intrusion Detection System,http://csrc.nist.gov/publication/nistpubs/800-31/sp800-31.pdf.

[20] Lundin, E., and Jonson, E., "Survey of Intrusion Detection Research", Technical Report 02-04, Chalmers University of Technology, Göteborg, Sweeden, 2001.

[21] Mé , L., and Michel, C., "Intrusion Detection: a Bibliograpy," Technical Report SSIR-2001-01, September,2001, SUPELEC, France.

[22] Lunt, T., Tamaru, T., Gilham, F., Jagannathan, R., Neumann, P., Javitz, H., Valdes, A., and Garvey, T., "A Real Time Intrusion Detection Expert System (IDES)", Final Technical Report, Computer Science Lab., SRI International, Menlo Park,, California, Feb., 1992.

[23] Porras, P.A., and Neumann, P.G., "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances", Proc. National Information Systems Security Confrenece, Baltimore, MD, Oct. 1997.

[24] Forrest, S., Hofmeyer, S.A., Somayaji, A., and Longstaff, T.A., "A Sense of Self for Unix Process", Proc. 1996 IEEE Symp. on Security and Privacy, pp. 120-128, 06-08 May 1996, Oakland,CA.IEEE Computer Security Press, Los Alamitos, CA.

[25] Cansian, A.M., "Desenvolvimento de um Sistema Adaptativo de Detecção de Intrus os em Redes de Computadores", PhD Thesis, Instituto de Física de São Carlos, USP, São Carlos, SP, 1997.

[26] Manikopoulos, C., and Papavassiliou,S., "Network Intrusion and Fault Detection: A Statistical Anomaly Approach", IEEE Communication Magazine, Vol. 40, No. 10, pp. 76-82, Oct 2002.

[27] Fink, G., Ko, C., and Levitt, K., "Automated Detection of Vulnerabilities in privileged Programs by Execution Monitoring", Proc. Of the 10th Annual Computer Security Apps. Conf., pp. 134-144, December 5-9, 1994.

[28] Mukkamala, S., Janoski, G., and Sung, A., "Intrusion Detection Using Neural Networks and Support Vector Machines", IEEE Proceedings, 2002.

[29] Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiwari, A., Yang, H., and Zhou, S., "Specification-based anomaly detection: a new approach for detecting network intrusions", In Proceedings of the 9th ACM Conference on Computer and Communications Security (Washington, DC, USA, November 18 - 22, 2002). V. Atluri, Ed. CCS '02. ACM Press, New York, NY.

[30] Sarasamma, S.T., Qiuming, A., and Huff, J., "Hierarchical Kohonenen Net for Anomaly Detection in Network Security", IEEE Trans. on System, Man, and Cybernetics – Part B, Cybernetics, Vol. 35, No.2, April 2005.

[31] Xiangyang Li, and Nong Ye, "A Supervised Clustering and Classification Algorithm for Mining Data with Mixed Variables", IEEE Trans. On Systems, Man, and Cybernetics, Part a: Systems and Humans, Vol. 36, No. 2, March 2006.

[32] Yu, B., Byres, E., and Howey, C., "Monitoring Controller's "DNA Sequence for System Security", *ISA Emerging Technologies Conference, Instrumentation Systems and Automation Society*, Houston, September 2001.

[33] Martinelli, M., Tronci, E., Dipoppa, E., and Balducelli, C., "Electric Power System Anomaly Detection Using Neural Networks", Lecture Notes in Computer Science, Vol.3213/2004, pp 1242-1248, Springer-Verlag, Heidelberg, Oct. 2004.

[34] Wang, W. and Battiti, R., "Identifying Intrusions in Computer Networks with Principal Component Analysis". Proceedings of the First International Conference on Availability, Reliability and Security (ARES 2006), IEEE press society, pp. 270-277, April, 20-22nd, Vienna, Austria.

[35] Song, D., Heywood, M.I., and Zincir-Heywood, A., "Training Genetic Programming on Half a Million Patterns: An Example from Anomaly Detection", IEEE Trans. On Evolutionary Computation, Vol. 9, No. 3, June 2005.

[36] Bigham, J., Gamez, D., and Ning Lu, "Safeguarding SCADA Systems with Anomaly Detection", V.Gorodetsky et al.(Eds.):MMM-ACNS 2003, LNCS 2776, pp. 171-182, Springer-Verlag Berlin Heidelberg, 2003.

[37] Pawlak, Z., "Rough Sets", International Journal of Information and Computer Sciences, Vol.11, pp. 341-356, 1982.

[38] Lambert-Torres, G., "Applications of Rough Sets in Power System Control Center Data Mining", IEEE Power Engineering Society Winter Meeting 2002, Vol. 1, pp. 627-631.

[39] Lambert-Torres, G. et al, "Power System Security Analysis Based on Rough Classification", Rough-Fuzzy Hybridization: New Trend in Decision Making, S.K. Pal & A. Skowron, Springer-Verlag Co., pp. 263-274, 1999.

A Extensão da Responsabilidade dos Provedores nos Crimes Contra a Honra

Luana Marasciulo Garcia, Marcos Cordeiro d'Ornellas, Quésia Falcão de Dutra, e Rafaela Mozzaquattro Machado, *Universidade Federal de Santa Maria*

***Abstract* — This article aims to determinate the extension of the responsibility of Internet providers in crimes against honor. This way the argument will be built to demonstrate the need of a specific law that regulates Internet crimes.**

***Palavras-chaves* — Crimes cibernéticos, provedores, responsabilidade.**

I. Introdução

A Internet constitui-se de um emaranhado de redes ao redor do mundo, não possuindo centro nem governo específico. Dessa forma, gera-se a necessidade de defender os direitos fundamentais, tais como privacidade, acesso a bases de dados sensíveis, confidencialidade e intimidade das pessoas, bem como de tutelar os direitos relativos à propriedade intelectual.

É uma entidade abstrata, não personificável, considerada o maior vetor de comunicação da atualidade. Sua evolução insere a sociedade em uma nova realidade transnacional, a qual apresenta uma problemática no contexto da sua regulamentação, merecendo, por isso, a tutela específica por parte do Direito.

O presente trabalho tem como escopo delinear os atores que promovem o acesso ao referido meio de comunicação e a extensão de sua responsabilidade no âmbito criminal.

Artigo recebido em 24 de Setembro de 2006. Este trabalho foi desenvolvido com apoio do Centro de Processamento de Dados, da Universidade Federal de Santa Maria.

Luana Marasciulo Garcia é acadêmica do Curso de Direito da Universidade Federal de Santa Maria, Santa Maria, Rio Grande do Sul, Brasil, e integrante do Legislation and Information Security Group (LegIS) (e-mail: mgluana@gmail.com).

Prof. Dr. Eng. Marcos Cordeiro d'Ornellas é orientador do Legislation and Information Security Group (LegIS) e do Multimedia Information Processing Group (PIGS), da Universidade Federal de Santa Maria, Santa Maria, Rio Grande do Sul, Brasil (e-mail: marcosdornellas@gmail.com).

Quésia Falcão de Dutra é acadêmica do Curso de Direito da Universidade Federal de Santa Maria, Santa Maria, Rio Grande do Sul, Brasil, e integrante do Legislation and Information Security Group (LegIS) (e-mail: quesia.fd@gmail.com).

Rafaela Mozzaquattro Machado é acadêmica do Curso de Direito da Universidade Federal de Santa Maria, Santa Maria, Rio Grande do Sul, Brasil, e integrante do Legislation and Information Security Group (LegIS) (e-mail: rafaela.mac@gmail.com).

II. Principais atores

Nesse paradigma, configuram-se como viabilizadores do uso da rede os provedores de serviço, os quais se subdividem, de acordo com sua função, em: *Backbone*, Acesso, Conteúdo, Informação, Hospedagem e Correio Eletrônico.

Provedores de *backbone* são as estrutura pela qual a Internet está ordenada. Também conhecidos como espinhas dorsais, são organismos físicos de rede capazes de manipular grandes volumes de informação. Conectados aos backbones estão os provedores de acesso. É destes provedores a responsabilidade de escolher a espinha dorsal a qual irão se conectar.

O provedor de *acesso* é um prestador de serviço técnico que coloca o servidor conectado permanentemente à Internet. Ele se mantém à disposição de seus assinantes para permitir-lhes a navegação, o acesso a páginas na Web, além do recebimento e envio de programas, arquivos e e-mails, entre outros. É atividade-meio, um contrato de serviço, sendo o provedor o fornecedor e o usuário final o consumidor.

O conteúdo das páginas na Internet é elaborado por editores de conteúdo, os quais podem ser empresas publicitárias, jornais, empresas comerciais, associações ou indivíduos que possuem páginas pessoais.

Geralmente, a página é hospedada em um provedor de *conteúdo*, o qual armazena dados para o acesso público.

Sabe-se que a rede de computadores permite a interação entre os usuários e os terminais do servidor remoto, outorgando serviços de correio eletrônico, dados multimídia, transferência de jogos, vídeos, imagens, etc. A operação da infra-estrutura que transporta a informação é conduzida por um conjunto de administradores de redes de telecomunicações. Em um nível internacional, a Internet está constituindo redes supranacionais conectadas entre si. Estas grandes redes estão, por sua vez, conectadas a outras redes em nível inferior, assim como as redes privadas conectadas à Internet chamadas Intranets.

De acordo com Marcel Leonardi: "*Provedor de hospedagem é a pessoa jurídica que fornece o serviço de armazenamento de dados em servidores próprios de acesso remoto, possibilitando o acesso de terceiros a esses dados, de acordo com as condições estabelecidas com o contratante do serviço*".

Já o provedor de *informação*, é aquele que coleta, mantém e organiza a informação através da Internet, para que seus

assinantes possam acessá-la. Tal provedor é seu autor, podendo fundir-se na mesma figura do provedor de conteúdo, no caso de também ser este autor da informação por ele disponibilizada.

Por fim, tem-se o provedor de *correio eletrônico*. Existem empresas que oferecem somente este serviço, ainda que grande parte dos provedores de acesso forneça, concomitantemente, contas de correio eletrônico. Basicamente, possibilita ao usuário o recebimento e o envio de mensagens eletrônicas.

Devido às peculiaridades na utilização de cada uma das figuras elencadas, surge uma nova relação, ainda não tutelada pelo Direito pátrio. Em decorrência desta relação, inúmeros riscos emergem para a sociedade como um todo. Apenas a título de exemplificação, cita-se a falta de controle na divulgação de material na Internet impróprio para crianças.

Mediante a análise da função de cada provedor, bem como as conseqüências resultantes dessa divisão, percebe-se a premente necessidade de proporcionar segurança e estabilidade na relação usuário-provedor. Frisa-se a facilidade que esse meio proporciona para a ocorrência de ilícitos civis e penais.

Nesse sentido, analisar-se-á casos específicos de ilícitos, quais sejam os crimes contra a honra, devido ao fato de serem os mais recorrentes neste meio em nosso país. Desde 2001, quando foi criada em São Paulo a 4ª Delegacia de Meios Eletrônicos da Divisão de Investigações Gerais do Departamento de Investigação sobre Crime Organizado, houve 1.200 inquéritos, a maioria relacionada a denúncias de crimes contra a honra, cometidos no site "Orkut", por meio dos denominados scraps (recados que um usuário envia a outro).

III. Os Crimes Contra a Honra

Os crimes contra a honra estão elencados no Capítulo V do Título I da Parte Especial do Código Penal Brasileiro, entre os artigos 138 e 140, dividindo-se, respectivamente, em calúnia, difamação e injúria.

A honra, segundo Victor Eduardo Gonçalves, "*é o conjunto de atributos morais, físicos e intelectuais de uma pessoa, que a tornam merecedora de apreço no convívio social e que promovem a sua auto-estima*". Conforme a doutrina, classifica-se a honra em objetiva ou subjetiva, sendo a primeira aquilo que os demais pensam a respeito do indivíduo, enquanto a segunda, o juízo que faz de si mesmo. Enquanto os crimes dos artigos 138 e 139 ofendem a honra objetiva da vítima, o definido pelo artigo 140 afronta a sua honra subjetiva.

Define-se a calúnia por imputar, *falsamente, fato definido como crime* a alguém, incluindo-se, ainda, neste tipo, aquele que sabendo falsa a imputação, a propala ou divulga, abrangendo, até mesmo, a calúnia contra os mortos. Consuma-se o delito no momento em que terceiro toma conhecimento da inculpação, exigindo-se o "plus" de que o fato imputado seja falso.

Todavia, admite-se a exceção da verdade, a qual consiste na ausência da tipicidade, caso se prove que o fato alegado pelo autor é verdadeiro, ficando este responsável pelo ônus probandi.

Já a difamação define-se como a imputação de *fato ofensivo à reputação* de outrem. Assim como no crime anterior, tem-se por consumado quando terceira pessoa souber da atribuição. Por sua própria natureza, aqui não interessa se o fato é falso ou não, pois o que se pretende reprimir é a propagação de fatos desabonadores. Dessa forma, não cabe, neste caso, a exceção da verdade como um meio de defesa do autor.

Por último, a injúria define-se pela *ofensa à dignidade ou decoro* de alguém. Trata-se de imputação não-fática, da imposição de qualidades negativas à pessoa. Consuma-se com a percepção da própria vítima a seu respeito.

Em comum entre os delitos contra a honra, têm-se os fatos de que: a) trazem a possibilidade de requisitar explicações, isto é, havendo qualquer incerteza da vítima acerca de ter sido ou não ofendida ou sobre o fidedigno sentido do que contra ela foi dito, poderá fazer requerimento ao juiz, o qual mandará notificar o autor da imputação a ser esclarecida e, obtendo ou não resposta, entregará os autos ao requerente, de modo que se, após isso, a vítima ingressa com queixa, o juiz analisará se recebe ou rejeita, levando em conta as explicações dadas e; b) a ação penal ser privada, exceto no caso de a ofensa ter sido feita contra a honra do Presidente da República ou chefe de governo estrangeiro, em que será pública condicionada à requisição do Ministro da Justiça; no caso de ofensa a funcionário público, sendo tal ofensa referente ao exercício de suas funções, sendo, então, pública condicionada à representação do ofendido e, por último, no caso em que da injúria real resultar lesão corporal, será pública incondicionada.

A pena pelos crimes contra honra vai de 6 meses a 2 anos de detenção e multa.

Sendo assim, todo e qualquer *modus operandi* capaz de consumar tais delitos é válido. Há, desta maneira, de se perceber que a Internet é um meio extremamente propício para o alastramento destes crimes, fazendo-se necessário, cada vez mais, que haja meios de inibi-los neste campo.

IV. A Extensão da Responsabilidade dos Provedores

No ordenamento jurídico brasileiro, não existe lei específica que regulamente as relações na Internet. Dessa forma, é preciso adequar o caso concreto à legislação vigente.

É justamente por esta lacuna no ordenamento que a responsabilidade dos provedores ainda é muito restrita.

Utilizar-se-á um caso específico para que se possa melhor elucidar a problemática. Quando, supostamente, alguém ofende a honra de outro indivíduo por meio de uma página da Internet, devem-se analisar certos requisitos.

Primeiramente, é necessário perceber-se de qual delito se trata, observando as peculiaridades de cada um.

Em segundo lugar, deve haver a individualização do ofendido, para que se possa perfectibilizar o crime contra a

honra. É essencial que haja uma vítima específica para configurar a ofensa.

Após o cumprimento destas duas etapas, inicia-se a busca pelo autor do fato delituoso. Neste momento, surge a responsabilidade do provedor. Quando requisitado pelo Poder Judiciário para que informe os dados do suposto autor, o provedor não pode se eximir de tal responsabilidade, tendo o dever de fornecer todos os dados que possuir para a identificação e qualificação do sujeito ativo.

Esta é a principal responsabilidade que pode ser atribuída aos provedores, pois o autor não pode se utilizar deles como um "manto de proteção" para que possa realizar práticas ilícitas.

Os provedores oferecem um serviço a seus consumidores, tendo o dever de possuir uma forma de identificá-los caso estes não tenham uma postura adequada, a qual deve ser consoante com os princípios que vigem na sociedade, sejam eles da ética e moral, bons costumes ou mesmo aqueles de cunho legal.

Por outro lado, quando se tratarem de crimes contra os Direitos Humanos no mundo virtual, o site provedor poderá ser responsabilizado de forma mais ampla, desde que saiba da existência do crime, ou seja, desde que haja comunicação por parte do Ministério Público ou de um popular.

Havendo esta comunicação, é mister que o provedor retire a ofensa da rede em um tempo razoável, podendo ser responsabilizado criminalmente se não o fizer.Frisa-se que não há uma definição legal do que é tempo razoável, devendo o aplicador da lei utilizar-se dos costumes e do bom-senso.

Assim, percebe-se que a extensão da responsabilidade dos provedores é bastante restrita, existindo apenas uma pequena exceção, qual seja: crimes contra os Direitos Humanos. É necessária a criação de uma lei específica que regulamente esta nova atividade, atribuindo direitos e deveres específicos a todos os entes participantes da relação, para que se possa ter uma maior segurança jurídica.

Referências Bibliográficas

[1] A. E. Pasqual, *Privacy in the next generation Internet: data protection in the context of the European Union,* PhD thesis, Royal Institute of Technology, Stockholm, Sweden, December 2002.

[2] A. J. Rover, *Direito e Informática*, Manole, Ed. Barueri, São Paulo, 2005.

[3] Brasil, *Código Penal*, Saraiva, Ed. São Paulo, 2006.

[4] Brasil, *Constituição Federal da República Brasileira*, Saraiva, Ed. São Paulo, 2006.

[5] C. R. Bitencourt, *Tratado de Direito Penal*, vol. 2, Saraiva, Ed. São Paulo, 2004.

[6] M. Leonardi, *Responsabilidade Civil dos Provedores de Serviço na Internet*, Juarez de Oliveira, Ed. São Paulo, 2005.

[7] http://www.denunciar.org.br/twiki/bin/view/SaferNet.

[8] http://www.advogado.adv.br .

Provas e contra-provas periciais nos casos de crime eletrônico: a capacidade da lei processual penal face ao princípio da ampla defesa.

Ariel G. Foina, *Doutorando, Universidad de Salamanca*

***Resumo*—O presente artigo, ao abordar a natureza da prova pericial e sua prática tanto na fase do inquérito quanto no decorrer da instrução criminal, suscita eventuais fragilidades de natureza processual, no caso de crimes eletrônicos puros. Aborda-se a constitucionalidade do uso da Lei 9296 na investigação e instrução de crimes eletrônicos bem como do rito da perícia no Código de Processo Penal quanto ao respeito ao princípio da ampla defesa. Após, conclui pela possibilidade de aplicação subsidiária do Código de Processo Civil ou da criação de juízos especializados em crimes eletrônicos e tecnológicos apontando eventuais problemas de ambas as soluções.**

***Palavras-Chave*—Direito Eletrônico, Crime Eletrônico, Processo Penal, Perícia, Provas Eletrônicas, Contra Prova Pericial**

I. Introdução

O presente artigo vem tratar do que Daoun[1] conceitua como crime de informática puro e que aqui tratamos como crime eletrônico puro, no caso, aqueles em que os bens jurídicos eletrônicos são meio e fim da conduta delitiva.

As ideias aqui propostas são decorrentes da experiência profissional do autor no campo da Advocacia em crimes eletrônicos, bem como, de dados obtidos em pesquisa de campo realizada no decorrer da elaboração de tese doutoral que trata da sub-cultura hacker e outras sub-culturas desviantes localizadas no ciberespaço brasileiro.

II. Da Perícia no Crime Eletrônico na Fase Inquisitorial

O inquérito policial é a fase do procedimento penal no direito brasileiro que precede o processo judicial. No inquérito, ao contrário do processo, o que se pressupõe como princípio orientador dos atos é o princípio do "*in dubio pro societate*", ou seja, na duvida se preza a defesa da coletividade em detrimento do réu.

Assim, nesta fase, nada mais natural do que termos o corpo administrativo do estado responsável pela condução do inquérito, seja a policia civil, federal, orientando seu trabalho para a busca de indícios e argumentos probatórios que busquem a condenação do réu. Esta orientação, de buscar a condenação do réu, é, por princípio jurídico, inversa à do processo penal, onde se busca a absolvição e em que a condenação pressupõe cumprimento de todos os elementos imprescindíveis para tal, via de regra, tipicidade, culpabilidade, nexo causal entre a conduta típica e a conduta do réu e culpabilidade.

Assim, falando-se especificamente da perícia, a linha investigativa da mesma dependerá da quesitação feita pela autoridade condutora do inquérito policial. A forma como se elaboram os quesitos determina a linha investigativa que o perito terá de adotar no decorrer do trabalho pericial.

Não é função do perito conduzir as investigações policiais. Na estrutura administrativa policial brasileira, não temos essa figura técnico-investigadora do "investigador de cena de crime" ou do "detetive cientifico"[2]. No Brasil, o que ocorre é que, as figuras responsáveis pela condução do inquérito (e também do processo, tema que será abordado mais adiante) não são portadoras de conhecimento técnico especializado. Desta forma, na prática, temos agentes policiais, e no caso de inquéritos de maior porte, os próprios delegados de polícia, responsáveis por elaborar quesitos e tomar decisões sobre a condução das referidas investigações, agentes e delegados estes os quais, diferentemente dos peritos, possuem uma formação deliberadamente focada nos aspectos jurídicos do inquérito e não nos aspectos da materialidade técnica do delito eletrônico.

É importante destacar o fato de que, dos crimes previstos no ordenamento jurídico brasileiro, dentre os que dependem de perícia para a efetiva constatação da materialidade, os crimes eletrônicos puros são, sem sombra de dúvida, os crimes onde a efetiva materialização do delito é de mais difícil constatação. Isso se dá devido a uma cultura instaurada dentre diferentes subculturas desviantes da Internet de sempre se tentar apagar os elementos probatórios que possam apontar a autoria (no caso de dano) ou a materialidade (no caso de acesso não autorizado ou de interceptação de comunicação informática) do delito perpetrado.

III. Do Procedimento Pericial no Processo Penal

Assim, vindo do procedimento inquisitorial, realizada sem acompanhamento da defesa do réu, a perícia é recebida no processo penal como mais um dos elementos que podem compor o livre convencimento do magistrado. Na legislação

Manuscrito recebido em 24 de setembro de 2006.

A. G. Foina é Doutorando pela Universidade de Salamanca no programa de Processos de Mudança na Sociedade Contemporânea, Sociólogo pesquisador da Cultura Hacker e Advogado com atuação na área do Direito Eletrônico. (arielfoina@gmail.com ou gomide@usal.es).

pátria só se admitem as provas produzidas no decorrer do processo judicial, de forma que, atos já praticados no inquérito, nos processos administrativos-disciplinares ou nas comissões de sindicância, dependem de ratificação ou de nova produção para que passem a compor o processo penal. Isso ocorre, especialmente com o interrogatório do réu e com o depoimento das testemunhas já ouvidas no inquérito.

Com os laudos periciais, é raro, na pratica jurisdicional, a determinação de que seja refeita a perícia anteriormente já produzida, o que se tem é a intimação dos peritos responsáveis pelo laudo para que os mesmos, na condição de testemunhas, reiterem o já contido no laudo produzido no âmbito do inquérito policial. Nestes casos, o que é possível de se fazer, tanto da parte da defesa do acusado, quanto do *parquet* ministerial, é a apresentação de quesitos novos aos peritos para que os mesmos se manifestem.

Ocorre porém que, uma vez que tanto as delegacias de polícia, sejam elas federais, civis ou administrativas, quanto os juízos penais e criminais, tem sua competência determinada, via de regra, pelo local da ocorrência do delito e a natureza jurídica da vítima. Dessa forma, é natural que, no decorrer do processo penal, a resposta a novos quesitos, e, inclusive, a realização de nova perícia, se for o caso, seja feita exatamente pelo mesmo órgão responsável pela elaboração da perícia no bojo do inquérito policial. Mais do que isso, dependendo da jurisdição, pela carência de peritos especializados em crimes eletrônicos, existe grande possibilidade de que a perícia venha a ser realizada pelo mesmo perito, funcionário do órgão técnico de determinada jurisdição.

IV.Da Perícia no Crime Eletrônico no Processo e dos Juízos Especializados

Assim, é nesse contexto que se deve inserir o debate referente a possibilidade e natureza da perícia dos crimes eletrônicos puros face ao nosso atual ordenamento jurídico.

Nosso foco de preocupação, no presente trabalho, são os crimes eletrônicos puros, assim, é de fundamental relevância o dado empírico já apresentado anteriormente de que a materialidade de tais delitos é de difícil constatação, em especial por determinados traços culturais intrínsecos aos grupos sociais de onde originam boa parte dos autores de tais delitos. Neste contexto, onde o autor do delito é portador de conhecimento técnico tal que é capaz de apagar rastros de acessos não autorizados e registros de entrada e saída de sistemas de forma a dificultar e até a inviabilizar a determinação da materialidade ou o estabelecimento de nexo causal, um dos recursos jurídicos mais importantes para o combate e investigação de tais delitos encontra-se nos mecanismos estabelecidos na Lei 9296 de 1996, que estabelece os procedimentos para a quebra de sigilo telefônico, telemático e informático.

Tal lei porém é um paradoxo jurídico que, por si só, enfraquece a investigação e a instrução processual para estes tipos de crimes. Sua ementa assim diz: "*Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal*", o referido inciso por sua vez afirma:

"*XII - é inviolável o sigilo da correspondência 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;* "(grifo nosso).

Assim, fica claro que a Carta Magna apenas permite, e a Lei 9296 apenas se propõe, à quebra de sigilo telefônico, descartando-se assim a correspondência, as comunicações telegráficas e de dados.

Porém, por paradoxal que é, a Lei 9296, no parágrafo único de seu artigo 1o traz:

"*Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática*".

Dessa forma, a Lei aqui tratada, quando utilizada para fins de investigação e instrução criminal, nos casos de crimes eletrônicos puros, abre ampla margem a questionamentos referentes a constitucionalidade, e por conseqüência, à validade das provas produzidas sob a égide do referido dispositivo legal, fragilizando assim a investigação e, por conseguinte, a obtenção da verdade real, princípio jurídico fundamental aos processos de natureza penal.

V.Da Contra Prova Pericial e da Ampla Defesa

Outro problema que merece destaque no que tange as perícias de crimes eletrônicos puros, visto o papel fundamental que tem para identificação de nexo de causalidade e de materialidade, nos referidos delitos, é a possibilidade de se ter respeitado o princípio constitucional e humano, do direito à ampla defesa, por parte do acusado.

No ordenamento jurídico brasileiro, quanto ao Código de Processo Penal, o perito, e por conseguinte, a perícia, respondem diretamente ao juízo, bem como, por decorrente dedução, a ambas as partes, tanto defesa quanto acusação, é o que decorre da análise do artigo 159 da referida carta legal, quando afirma:

"*Art. 159. Os exames de corpo de delito e as outras perícias serão feitos por dois peritos oficiais*".

Porém, a jurisprudência entende que, face ao princípio do livre convencimento do juiz, não basta apenas a constatação, por parte do perito do juízo, de uma eventual autoria ou materialidade em determinado delito, há ainda a necessidade de o perito apresentar os elemento que fundamentam seu parecer, os quais, no caso de crimes eletrônicos puros, são, em sua grande maioria, decorrentes de uma análise sistêmica de difícil explicação para pessoas não técnicas, ou, decorrente de dados de programas cuja juntada, em forma documental, fica prejudicada. Para exemplificar tal situação, temos, a

hipótese de uso de detectores de intruso (IDS) e de seus relatórios para fundamentar um nexo de autoria, ou, o uso de analisadores de pacotes para identificar a violação ou o dano a determinado sistema de redes. Em ambos os casos, os registros decorrentes do uso de tais ferramentas, mesmo que claros a um perito de formação técnica, são praticamente ilegíveis a pessoas sem a devida formação, em especial, a média dos delegados e juízes que atualmente atuam no sistema penal brasileiro.

Desta forma, sendo o perito, no caso específico do processo penal brasileiro, figura vinculada direto e exclusivamente ao juiz, não é possível, face nosso atual ordenamento jurídico, a execução de perícia por parte da defesa, ou, se quer, a indicação de assistente técnico da defesa para acompanhar os trabalhos realizados pelo perito oficial, o que torna difícil, o devido exercício do princípio da ampla defesa, uma vez que o próprio advogado de defesa, via de regra, não tem conhecimento técnico o suficiente para, se quer, questionar os fundamentos da decisão do perito na resposta dos quesitos apresentados.

Nota-se que, ao tratar a perícia, o Código de Processo Civil a situa no Capítulo II do Título VII do seu primeiro livros, capitulo esse intitulado como "*Do exame de corpo de delito e das perícias em geral*". É de suma importância frisar que as preocupações aqui apresentadas são decorrentes da complexidade dos elementos formadores do convencimento do perito quanto as fatos juridicamente relevantes nos casos de crimes eletrônicos puros, pois, em tais, não se pode transferir ao perito, responsabilidade que é, por direito e dever, de competência personalíssima do Juiz de decidir a lide.

VI. Possíveis Soluções à Questão

Não obstante a tal, não há, apesar de desejada, a necessidade de um diploma legal específico para tratar do processo no caso de crimes eletrônicos puros e outros delitos tecnológicos, sendo passíveis, sob a égide do nosso atual ordenamento jurídico, duas soluções que passaremos a apresentar.

Primeiramente, reconhecida pelo juízo a complexidade da matéria e a lacuna da lei penal, poder-se-ia aplicar, subsidiariamente, o Código de Processo Civil, assim como se faz em complementação ao processo trabalhista nos casos de perícia.

A aplicação subsidiária do CPC abriria a possibilidade de indicação de assistente técnico, por parte da defesa, para acompanhar os trabalhos periciais, ou, em se tratando de re-perícia ou perícia de contra prova, por exemplo, da pactuação entre Defesa e Ministério Público de eventual instituto ou pessoa técnica de notório saber na área, distinta daquela responsável pela elaboração do primeiro laudo, para formulação de um novo, desde que aprovado pelo Juiz.

Esta solução, se por um lado torna inquestionável o respeito ao princípio da ampla defesa, por outro lado, se vista de uma perspectiva mais pragmática, gera dificuldades que podem vir a influenciar o resultado da referida perícia, dependendo do nível técnico e da natureza da investigação se levamos em conta a doutrina pericial da "cadeia de custódia"[3] que preza pelo controle da prova científica colhida em loco. No caso de outro que não um instituto de criminalística com fé pública ou mesmo, no caso de acompanhamento dos trabalhos por assistente pericial, haveria a necessidade de se trabalhar sobre cópias do material colhido, o que, em se tratando, por exemplo, de tentativa de recuperação de dados em superfície logicamente desmagnetizada tornaria o trabalho impossível ou permitiria, a depender do caso fático, uma contaminação irreversível da amostra.

A segunda solução proposta, é, por um lado, menos complexa, do ponto de vista técnico-legal, porém, de uma dificuldade política extremamente superior. Trata-se da criação de juízos especializados com Juízes de primeira e segunda instâncias com formação técnica suficiente para que os mesmos tenham capacidade de não apenas compreender os laudos periciais, quanto, de apreciar por si mesmos os arquivos e registros que venham fundamentar as respostas do perito.

Tal solução não só reduziria o prejuízo ao princípio da ampla defesa, como, retiraria da prova pericial a carga de ser elemento probatório crucial nos processos aqui em questão, uma vez que permitiria, em casos extremos, a própria inspeção judicial.

A resistência política se dá, porém, devido a necessidade de se compor todo um corpo jurídico, seja de Magistrados, seja de membros do Ministério Público, e até mesmo de Advogados, com tal tipo de formação multidisciplinar. Tal resistência, porém, não carece de outros argumentos que não o meramente político e encontra forte fundamento em dispositivos da doutrina do Direito, quando da interpretação do princípio jurídico do Juiz Natural, bem como do princípio doutrinário da avaliação das condutas sob a ótica do comportamento do "homem médio"

VII. Conclusões

Assim, até o presente momento, fica sem solução a questão aqui apresentada, o que, por hora, não é geradora de maiores preocupações uma vez que, a atual legislação penal brasileira prevê a aplicação efetiva de muitos poucos tipos penais às condutas tidas como crimes eletrônicos puros, em especial o tipo penal do Dano, e o da Interceptação de Comunicação, artigos 163 do Decreto 2848 e 10 da Lei 9296 respectivamente.

Porém, visto que encontra-se em tramitação diferentes projetos de lei com vistas a adicionar os mais diferentes tipos penais decorrentes de delitos eletrônicos puros ao nosso Código Penal, a notória ausência de uma legislação processual que acompanhe os mesmos é preocupante e põe em questão a eficácia de tais normas vindouras.

Referências

[1] DAOUM, Alexandre Jean. “Crimes Informáticos” in BLUM, Renato Opice (org), *Direito Eletrônico: A Internet e os Tribunais*, Bauru: Edipro, 2001.

[2] no uso original do termo Crime Scene Investigator e Forensic Detective

[3] no uso original do termo Chain of Custody

Ariel G. Foina é Doutorando pela Universidade de Salamanca no programa de Processos de Mudança na Sociedade Contemporânea, Sociólogo pesquisador da Cultura Hacker e Advogado com atuação na área do Direito Eletrônico. É bacharel e licenciado em Ciências Sociais pela Universidade de Brasília e detém atualmente Diploma de Estudios Avansados em Sociologia pela Universidad de Salamanca aonde desenvolve tese doutoral cujo objeto são as sub-culturas desviantes do ciberespaço, especialmente no Brasil.

No ano de 2005, foi membro de Research Cluster sobre Tecnologia e Ação Social junta à Sheffield Hallam University na Inglaterra além de participar do PhD Forum do Human-Computer Interface Issues in e-Democracy do grupo Toward Electronic Democracy da Manchester Business School.

Dr. Foina é advogado inscrito na Seccional do Distrito Federal da Ordem dos Advogados do Brasil e tem diversas publicações na área de Direito Eletrônico, Cultura Hacker, Sociologia do Desvio e do Crime, além de trabalhar com pesquisas e projetos sociais na área de extensão universitária e educação.

“Grampos Digitais” Utilizando Software Livre

Ricardo Kléber Martins Galvão, Naris, Superintendência de Informática, UFRN

***Resumo*—Na apuração de crimes digitais e, mais especificamente, de crimes praticados utilizando microcomputadores, geralmente utilizam-se técnicas post-mortem, nas quais o sistema é periciado após o desligamento da máquina, cabendo ao perito a duplicação das mídias e avaliação de evidências armazenadas e/ou recentemente apagadas. Em muitos casos porém, (especialmente quando a máquina está conectada à Internet), para a realização da coleta de evidências é necessária a interceptação (“grampo”) dos dados em “tempo-real”, ou seja, a captura dos dados deve ser realizada com a máquina ligada e em utilização pelo(s) indivíduo(s) investigado(s). Este artigo tem por objetivo apresentar técnicas eficazes de captura e análise de tráfego (não encriptado) para utilização em casos de perícia envolvendo a utilização de microcomputadores ligados em rede. As ferramentas apresentadas são baseadas em software livre, isto é, sem custo adicional de software, perfeitamente aplicáveis nesta situação, além de adequadas a todos os orçamentos previstos para a atividade pericial.**

***Index Terms*—Computer Forensics, Network Security**

I. Definições na Área de Perícia Forense Aplicada à Informática

As investigações periciais em sistemas computacionais utilizam alguns termos, conforme definidos a seguir:

A. Perícia Forense Aplicada á Informática

Também conhecida como processo de análise de provas digitais ou análise de mídias informáticas, pode ser definido como o processo de extrair de sistemas computacionais dados que valham como prova.

1) Mídia de provas

O objeto (físico) real da investigação, isto é, o equipamento (e seus periféricos) que podem conter as provas procuradas, como arquivos armazenados em disco ou memória ou responsável pelo recebimento/geração de dados trafegados em rede quando estes forem os objetos da investigação.

2) Mídia de destino

O destino dos dados capturados e/ou copiados da mídia de provas. É a imagem pericial sobre a qual serão realizados os procedimentos de análise e busca por provas.

3) Análise ao Vivo

Análise realizada durante os procedimentos de coleta de dados (em tempo real), isto é, diretamente sobre a mídia de provas ou sobre o tráfego capturado de/para ela.

4) Análise Off-Line

Análise feita sobre a mídia de destino após a coleta de dados a partir da máquina e/ou rede investigada..

II. Preservação de “Local de Crime”

Na perícia forense tradicional, a preservação de “Local de Crime” consiste em isolar fisicamente todo o perímetro que contorna o ambiente em que foi praticado o delito de modo a preservar evidências, isto é, evitar que alguém possa manipular os componentes que serão periciados sem os cuidados recomendados.

Na perícia forense computacional, o “Local de Crime” é praticamente todo virtual, isto é, apesar dos componentes físicos utilizados para a prática do delito (microcomputador e periféricos a ele conectados), todos os indícios necessários estão em nos dados armazenados no interior da CPU em seu disco rígido e, em alguns casos, na memória principal.

III. Coleta de Evidências

Embora a definição de coleta de evidências seja bastante abrangente, já que engloba aspectos relacionados ao ambiente periciado, ferramentas e técnicas utilizadas para esta coleta, para este artigo, o procedimento de coleta de evidências restringir-se-á às modalidades relacionadas à captura de dados via rede, isto é, gerados a partir de uma máquina e/ou rede investigada e coletados utilizando "grampos" na rede utilizada para a comunicação.

Para a utilização dos conceitos apresentados neste artigo, supõe-se a autorização total para a interceptação de conteúdo das comunicações entre as máquinas das redes envolvidas (em todos os níveis da pilha de protocolos TCP/IP). A autorização total é necessária já que, em determinados casos, somente a interceptação de informações de transações (cabeçalhos dos pacotes) são autorizadas, impedindo o acesso aos dados dos usuários (necessários a este tipo de "grampo"), restringindo os resultados da coleta a determinação da origem e destino das comunicações.

A. Ferramentas Utilizadas

1) Tcpdump

Ferramenta para operação em modo texto que funciona como sniffer, capturando todos os pacotes que se apresentem os elementos da filtragem especificada em seus parâmetros de configuração de consulta.

Esta ferramenta será apresentada exclusivamente como mecanismo de captura de pacotes e geradora de arquivo binário para utilização pelo Wireshark.

2) Wireshark

Ferramenta em modo gráfico que tanto funciona como sniffer capturador de pacotes, como analisador de pacotes off-line (aceitando o padrão gerado pelo tcpdump por exemplo) e remontador de Streams TCP.

B. "Grampos" Digitais Utilizando Sniffers

Um sniffer é um hardware ou software que intercepta passivamente os pacotes que passam por uma rede. Os sniffers mais comuns são programas que permitem a uma placa de interface de rede (NIC) processar pacotes destinados a várias máquinas diferentes. Os sniffers baseados em software funcionam pondo o adaptador de rede em "modo promíscuo", que tem esse nome por aceitar todo o tráfego com o qual tem contato.

A instalação de sniffers tem por objetivo capturar todo o tráfego em uma rede, mesmo que o endereço de destino não seja o da máquina onde o sniffer está instalado.

Para realizar esta captura têm-se, basicamente, dois cenários:

1) O Sniffer Instalado em uma Rede Baseada em Hubs

2) O Sniffer Instalado no Roteador

O Roteador é o equipamento responsável pelo repasse de pacotes de/para a rede, ou seja, realiza a "ponte" entre uma rede e outra (uma Intranet e a Internet, ou entre duas redes internas por exemplo).

A instalação de um sniffer no roteador principal de uma rede investigada possibilita tanto a captura de todos os pacotes com origem na máquina/rede investigada destinados à rede externa como dos pacotes vindos da rede externa e destinados à rede/máquina investigada.

Em se tratando de uma atividade pericial, devidamente autorizada, e a conseqüente liberação de acesso a este equipamento para a instalação do sniffer esta operação independe da estrutura de conectividade da rede investigada, já que neste caso não importa se a rede utiliza hubs ou switches, a informação é coletada diretamente no roteador.

Dois são os problemas que podem surgir com esta modalidade de "grampo"

a) Embora um grande número de redes utilize microcomputadores com duas ou mais interfaces de rede para realizar a função de roteamento (ambiente ideal para a instalação do sniffer), algumas redes optam pela utilização de roteadores convencionais, isto é, equipamentos específicos para a função de roteamento, não permitindo a instalação de softwares como um

sniffer. Neste caso, é aconselhável que uma outra máquina (roteador) seja instalada entre o roteador e a intranet para forçar o tráfego a passar por este equipamento onde, finalmente, deve ser instalado o sniffer.

b) A atividade de roteamento demanda processamento e memória do equipamento, além do atraso gerado pela análise dos pacotes antes do encaminhamento ao destino, transformando os roteadores em "gargalos" naturais. A instalação de outros softwares (como um sniffer) nestes equipamentos, dependendo do volume de tráfego, pode significar um retardo adicional no encaminhamento de pacotes tal que inviabilize a operação ou, pelo menos, altere o comportamento normal da rede com relação ao acesso externo, podendo, assim, levantar suspeitas por parte dos investigados.

C. "Grampos" Digitais Utilizando Cópias de Pacotes a partir do Roteador

Este tipo de grampo consiste em retirar uma cópia de cada pacote que passa pelo roteador e enviá-la a uma rede/máquina para análise posterior.

O Netfilter/Iptables, solução de firewall utilizado por padrão nas novas versões do sistema operacional Linux suporta módulos em forma de extensão ao modelo original, permitindo a manipulação das mensagens que passam pelo roteador/firewall de acordo com necessidades específicas.

Para a realização da cópia de cada pacote que atravessa o roteador/firewall Linux baseado em Netfilter/Iptables, pode-se utilizar a extensão --ROUTE desenvolvida por Cédric de Launois, ainda em fase experimental mas bastante estável utilizada inicialmente para realizar reroteamento, ou seja, alterar a tabela de rotas de cada pacote reroteando-o para outra rede ou máquina.

O parâmetro --tee, desenvolvido por Patrick Schaaf, adicionado a esta extensão permite que o firewall/roteador realize o roteamento dos pacotes sem interferência direta, mas, retire uma cópia de cada um deles enviando-as para uma rede ou máquina específica.

Uma linha de exemplo para este tipo de "grampo" seria um cenário em que todos os pacotes destinados à servidores Web (porta 80/TCP) ao passar pelo roteador seriam copiados para a máquina 10.10.10.10 antes de serem submetidos a outras regras de filtragem/roteamento:

```
iptables -A PREROUTING -t mangle -p tcp --dport 80 -j
            ROUTE --gw 10.10.10.10 --tee
```

Assim, todo o tráfego Web seguiria até o seu destino, sem retardo adicional, porém todos os pacotes seriam copiados para uma máquina específica onde seria realizada a perícia posteriormente.

Para a utilização desta extensão, porém, é necessária a aplicação de um patch específico no kernel do Linux e no próprio Iptables, além da recompilação de ambos para a ativação da nova funcionalidade.

IV. Análise de Evidências

Desviando via Netfilter/Iptables/ROUTE/tee todos os pacotes vindos da rede/máquina investigada para uma estação pericial, ferramentas específicas são então utilizadas para realizar a separação de tráfego em arquivos específicos para a análise posterior.

A. Ferramentas Utilizadas

Para a coleta de dados a ferramenta utilizada é a tcpdump, gravando em formato binário (parâmetro -w). Para a leitura (remontagem de sessão) utiliza-se a ferramenta Wireshark, funcionalidade Follow TCP Stream.

B. Separando e Analisando Tráfego Telnet

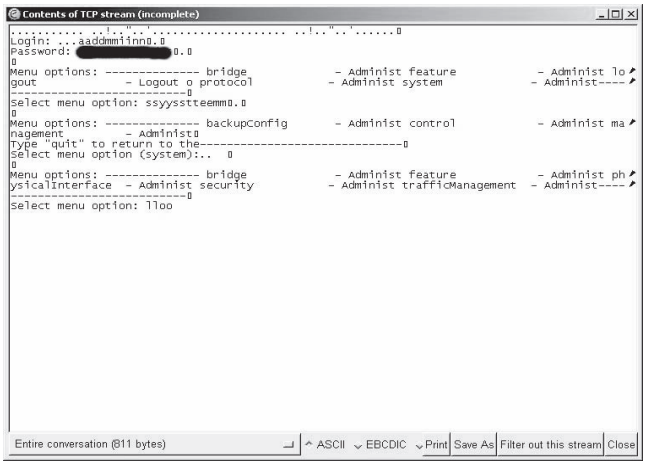
O Telnet é um protocolo de comunicação remota em modo texto que, por padrão, não utiliza encriptação dos dados, sendo, portanto, vulnerável a "grampos". Mesmo as senhas dos usuários de comunicações remotas via telnet podem ser facilmente capturadas por um "grampo".

Para realizar a separação do tráfego Telnet dos demais, na estação pericial, basta aplicar um filtro utilizando o tcpdump selecionando apenas os dados com origem ou destino à porta 23/TCP.

```
tcpdump –X –v –i <interface> port 23 -w
          <arquivo_específico>
```

A análise deste tipo de tráfego em “grampos” nem sempre apresenta resultados consistentes, já que não é um protocolo utilizado por usuários com pouco conhecimento técnico e, mesmo os usuários com um maior conhecimento técnico que desejam realizar comunicação remota em modo texto têm optado por utilizar o SSH, protocolo semelhante, porém, com tráfego de dados e autenticação encriptados, isto é, imune a “grampos”.

A análise apresentada a seguir é feita utilizando o Wireshark e remontando as sessões Telnet encontradas no arquivo gerado pelo tcpdump.



Neste caso a seção capturada apresenta o Login e senha (Password) para acesso a algum ativo de rede baseado em menus. Os caracteres aparecem duplicados pelo “echo” do Telnet.

C. Separando e Analisando Tráfego Web (HTTP)

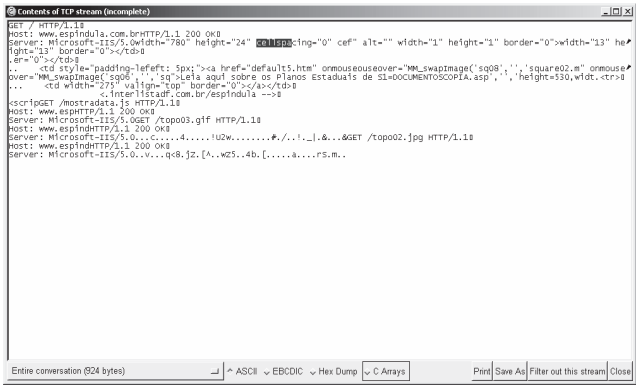
O HTTP é um dos protocolos de comunicação mais utilizados por usuários de todos os níveis e, apesar disso, não utiliza encriptação dos dados, sendo, portanto, vulnerável a “grampos”. Mesmo as senhas dos usuários de comunicações remotas via HTTP podem ser facilmente capturadas por um “grampo”.

Para realizar a separação do tráfego HTTP dos demais, na estação pericial, basta aplicar um filtro utilizando o tcpdump selecionando apenas os dados com origem ou destino à porta 80/TCP.

```
tcpdump –X –v –i <interface> port 80 -w
          <arquivo_específico>
```

A análise deste tipo de tráfego em “grampos” pode ser inviabilizada se o usuário utiliza, para a navegação Web, ao invés do protocolo HTTP o HTTPS, protocolo semelhante, porém, com tráfego de dados e autenticação encriptados, isto é, imune a “grampos”.

A análise apresentada a seguir é feita utilizando o Wireshark e remontando as sessões HTTP encontradas no arquivo gerado pelo tcpdump.



Neste exemplo específico, a remontagem de pacotes envolvidos na comunicação apresentam detalhes sobre um site acessado pela máquina investigada (endereço, sistema operacional do servidor e detalhes sobre a página visitada)

D. Separando e Analisando Tráfego FTP

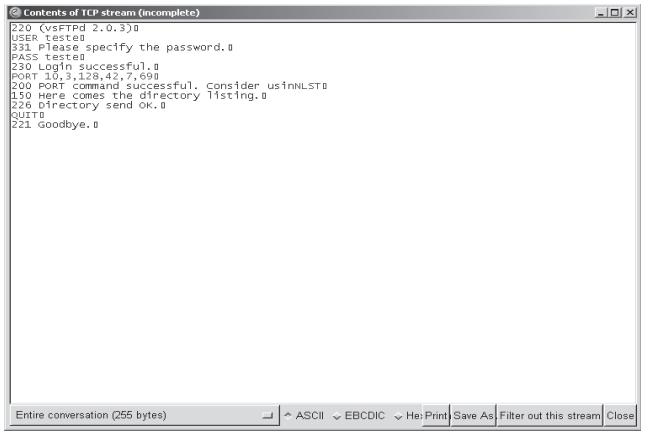
O FTP é um protocolo de comunicação bastante utilizado para transferência de arquivos entre máquinas via rede e, apesar disso, não utiliza encriptação dos dados, sendo, portanto, vulnerável a “grampos”. Mesmo as senhas dos usuários de comunicações remotas via FTP podem ser facilmente capturadas por um “grampo”.

Para realizar a separação do tráfego FTP dos demais, na estação pericial, basta aplicar um filtro utilizando o tcpdump selecionando apenas os dados com origem ou destino às porta 21/TCP e 20/TCP.

```
tcpdump –X –v –i <interface> port 20 or
    port 21 -w <arquivo_específico>
```

A análise deste tipo de tráfego em “grampos” pode ser inviabilizada se o usuário utiliza, para a transferência de arquivos via rede, ao invés do protocolo FTP o SCP, protocolo semelhante, porém, com tráfego de dados e autenticação encriptados, isto é, imune a “grampos”.

A análise apresentada a seguir é feita utilizando o Wireshark e remontando as sessões FTP encontradas no arquivo gerado pelo tcpdump.



Neste exemplo específico, a remontagem de pacotes envolvidos na comunicação apresentam Login do usuário (USER), senha (PASS) e comando digitado, neste caso, o usuário apenas solicitou a listagem de diretórios na máquina remota.

E. Separando e Analisando Tráfego de E-mails (SMTP, POP3 e IMAP)

Os protocolos relacionados ao serviço de Correio Eletrônico são, sem dúvida, os mais utilizados por usuários de todos os níveis e, apesar disso, não utilizam encriptação dos dados, sendo, portanto, vulnerável a “grampos”. Mesmo as senhas dos usuários de comunicações remotas via POP3 ou IMAP podem ser facilmente capturadas por um “grampo”.

Para realizar a separação do tráfego SMTP dos demais, na estação pericial, basta aplicar um filtro utilizando o tcpdump selecionando apenas os dados com origem ou destino à porta 25/TCP.

Para realizar a separação do tráfego POP3 dos demais, na estação pericial, basta aplicar um filtro utilizando o tcpdump selecionando apenas os dados com origem ou destino à porta 110/TCP.

Para realizar a separação do tráfego IMAP dos demais, na estação pericial, basta aplicar um filtro utilizando o tcpdump selecionando apenas os dados com origem ou destino à porta 143/TCP.

```
tcpdump –X –v –i <interface> port 25 or
        port 110 or port 143 -w
          <arquivo_específico>
```

A análise deste tipo de tráfego em “grampos” pode ser inviabilizada se o usuário utiliza envio autenticado de e-mails, além dos protocolos de recebimento POP3s e IMAPs, protocolos semelhantes, porém, com tráfego de dados e autenticação encriptados, isto é, imune a “grampos”.

Neste caso o Wireshark pode ser utilizado para remontar seções SMTP capturadas via tcpdump e verificar todos os e-mails enviados, com o Endereço IP de origem e endereço de e-mail de destino.

A remontagem de seções POP3 ou IMAP apresentam (ambas) informações de Login/Senha dos usuários que executarem estes serviços.

V. Considerações Finais

A falta de recursos financeiros para a compra de *softwares* comerciais para a realização de perícias em crimes digitais não representa de fato um problema atualmente pela diversidade e robustez das soluções disponíveis baseadas em *software* livre.

Esta apresentação demonstra com detalhes que todos os recursos necessários para a coleta de evidências digitais em “tempo real” estão disponíveis sem custo algum de *software*, muito embora existam soluções comerciais equivalentes, além de custos com treinamentos para utilização destas ferramentas.

References

[1] MANDIA, Kevin, PROSISE Chris, Incidence Response: Investigating Computer Crime, Osborne/McGraw-Hill, 2002.

[2] CASEY, Eoghat, Digital Evidence and Computer Crime, Academic Press, 2004.

[3] SHINDER, Debra L., Scene of the Cybercrime: Computer Forensics Handbook, Ed. Titel, 2002.

[4] Homepage do Projeto Netfilter/Iptables : http://www.netfilter.org

[5] Homepage do Tcpdump/Libpcap : http://www.tcpdump.org

[6] Homepage do Analisador de Protocolos de Rede Wireshark: http://wireshark.org

SuRFE – Sub-Rede de Filtragens Específicas

Ricardo Kléber Martins Galvão, PPGEE, UFRN
Sergio Vianna Fialho, PPGEE, UFRN

***Resumo*—O aumento do número de ataques a redes de corporativas tem sido combatido com o incremento nos recursos aplicados diretamente nos roteadores destas redes. Nesse contexto, os firewalls consolidaram-se como elementos essenciais no processo de controle de entrada e saída de pacotes em uma rede. Estes mecanismos de filtragem têm evoluído conforme evoluem as técnicas de ataques, chegando ao topo da pilha TCP/IP ao incorporar filtragens em nível de aplicação. Esta solução embora eficiente do ponto de vista do nível de filtragem, além de provocar um retardo natural nos pacotes analisados, compromete o desempenho da máquina na filtragem dos demais pacotes pela natural demanda por recursos da máquina para este nível de filtragem. Este artigo apresenta os resultados de um estudo de modelos de tratamento deste problema baseados no reroteamento de pacotes específicos para análise em uma sub-rede de filtragens específicas.**

***Index Terms*—Network Security**

I. Introdução

Acompanhando a evolução histórica dos *firewalls*, observa-se a rápida incorporação de novos mecanismos de filtragem, flexibilização de parâmetros de implementação e modularização de seus componentes, buscando dotar estes elementos periféricos de segurança de um maior grau de controle e bloqueio de ataques aos servidores e às estações por ele protegidos.

A necessidade de filtros específicos para determinados serviços que analisassem não só dados de encaminhamento de pacotes em nível de rede e transporte, mas que identificassem e bloqueassem ataques direcionados à própria aplicação, deram origem aos proxies.

A adição um *proxy* para cada porta relacionada a um serviço específico em execução tornou-se insuficiente, contudo, com o surgimento de aplicativos *peer-to-peer* para troca de arquivos entre máquinas de usuários conectadas à Internet. Esses aplicativos, embora inicialmente padronizados para acesso a partir de portas específicas, e assim poderiam ter seu tráfego bloqueado na filtragem em nível de transporte, passaram a utilizar portas aleatórias, demandando uma solução que investigasse os pacotes em nível de aplicação para identificar o tráfego gerado por este tipo de aplicação.

A incorporação dos proxies à máquina do *firewall*, por si só, representa um aumento natural do retardo no repasse dos pacotes, comprometendo em alguns casos, dependendo do volume de informações analisadas, a disponibilidade da máquina pelo aumento do uso dos recursos da máquina. O risco de comprometimento da máquina em que o *firewall* está em execução aumenta consideravelmente com a incorporação de proxies P2P, tornando-se uma decisão questionável a sua implementação em detrimento das implicações a ela inerentes.

Este artigo apresenta modelos para tratamento de tráfegos específicos baseando-se na utilização de uma sub-rede de filtragem e, assim, aliviando o volume e o nível de informações analisadas pelo *firewall* principal da rede.

II. Firewalls

O *firewall* é uma barreira inteligente entre a rede local da corporação e a Internet, através da qual só passa tráfego autorizado [6].

O motivo principal da instalação de *firewalls* é o controle de acesso em nível de *kernel* [5], realizando a filtragem antes, durante e/ou após o processo de roteamento dos pacotes.

A. Evolução dos Firewalls

1) Primeira Geração – Filtragem de Pacotes

O papel do *firewall* na filtragem de pacotes tradicional era o de assumir as regras de filtragem dos roteadores (*Access Lists* - ACLs), de modo a aliviar o volume de processamento nesses roteadores, isentando-os da responsabilidade pela análise e bloqueio de determinados pacotes.

A utilização de *firewalls* desta geração também se justificava em função das limitações encontradas no uso de ACLs em roteadores: interface de configuração pouco amigável, impossibilidade de registro local de *logs* de acesso/bloqueio, além de questões administrativas envolvendo interesses distintos entre corporações. No cenário mostrado na Figura 1, um roteador serve a duas redes com administradores diferentes e, conseqüentemente, o acesso às regras do roteador implicaria em compartilhamento da sua senha de administração. Caso esse acesso não fosse possível, o administrador em questão não poderia inserir regras de filtragem específicas para sua rede.

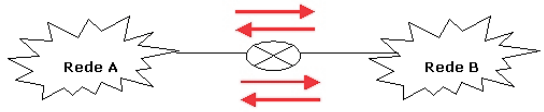


Fig. 1. Conexão de redes com roteador e sem *firewalls*

Uma alternativa a esse cenário seria uso de dois *firewalls* (entre as redes internas e o roteador) sob responsabilidade da administração local de cada uma destas redes. Essa solução além de "desafogar" o processamento do roteador, tornaria mais seguro e controlado o acesso ao equipamento de segurança e permitiria a inserção de regras específicas para cada rede no respectivo *firewall* local (Figura 2).

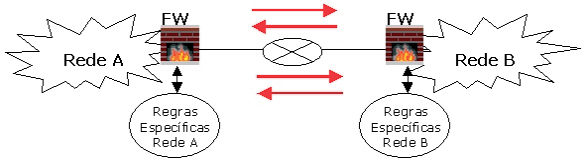


Fig. 2. Conexão de redes com roteador e com *firewalls*

2) Segunda Geração – Incorporação de NAT (*Network Address Translation*)

A segunda geração dos *firewalls* caracterizou-se pela incorporação de uma técnica de conversão de endereços (NAT) à máquina do *firewall*. Na implementação de alguns sistemas operacionais, as tarefas de NAT e filtragem de pacotes, embora na mesma máquina, eram realizados por ferramentas distintas, enquanto em outras implementações, uma mesma ferramenta realizava ambas as tarefas.

A partir de então, o uso de mascaramento (*masquerade*) de endereços IP privados para acesso à rede externa, utilizando temporariamente um único endereço externo (NAT N:1) passou a ser uma nova funcionalidade dos *firewalls*.

A conversão direta e fixa de endereços públicos em privados (NAT 1:1), em que determinadas máquinas da rede interna (geralmente servidores de aplicação) poderiam ser acessadas a partir da rede externa através de seu endereço público (mapeado para seu endereço privado) também fazia parte desta solução, e se encontrava disponibilizada a partir de então.

3) Terceira Geração – Checagem de Estados

Dentre as soluções existentes até então, a dificuldade dos *firewalls* era diferenciar os pacotes que entravam na rede como resposta a solicitações internas, dos pacotes que, partindo da rede externa, buscavam iniciar conexões em máquinas da Intranet.

A inspeção do estado dos pacotes (*stateful inspection*) marcou uma nova era para os *firewalls*. Sua terceira geração, com a possibilidade de restringir o acesso de pacotes vindos da rede externa, liberando aqueles relacionados a conexões estabelecidas a partir de máquinas internas e bloqueando os demais. Dessa forma, tornou-se possível evitar vários tipos de ataques conhecidos até então, aumentando consideravelmente a segurança da rede corporativa.

4) Quarta Geração – Filtragens Específicas em Nível de Aplicação

Antes do surgimento desta modalidade de filtragem, uma das maiores limitações para os *firewalls* na detecção e bloqueio de ataques contra redes corporativas eram os ataques contra as implementações de serviços liberados pelo *firewall*, ou seja, a exploração de vulnerabilidades nas aplicações em execução acessadas a partir de portas válidas (serviços tradicionais), utilizadas para prover acesso a partir de máquinas externas a informações da instituição.

Nestes casos específicos, informações como endereços IP, portas, protocolos e estados de conexão não eram suficientes para identificar e eventualmente bloquear a exploração das vulnerabilidades dos programas.

O "mito" de que os dados da camada de aplicação só deveriam ser manipulados pelos equipamentos das extremidades da conexão (cliente e servidor) caiu por terra, diante da necessidade de filtragem das informações transportadas nesta camada, de modo a identificar ataques em andamento contra a corporação.

A quarta geração de *firewalls* é marcada, portanto, por implementações que disponibilizam parâmetros para configuração de filtragem neste nível específico.

Proxies de Aplicação

A utilização dos proxies de aplicação consiste em dotar a rede de um elemento intermediário entre os usuários e os servidores de determinada(s) aplicação(ões). Este elemento recebe a solicitação de conexão a uma máquina externa e, ao invés de repassar o pacote, assume a condição de cliente iniciando uma nova conexão ao destino e repassando os pacotes de retorno ao cliente original.

A utilização deste tipo de serviço, além de proteger os endereços reais das máquinas internas (clientes), permite a filtragem e eventual necessidade de bloqueio de pacotes baseando-se em informações de seu cabeçalho IP, ou mesmo no conteúdo dos pacotes.

A grande desvantagem na adoção deste modelo é a necessidade de utilização de proxies específicos para cada serviço (http, smtp, ftp, etc.).

Firewalls de Aplicações

Os *firewalls* de aplicações têm funcionalidades semelhantes aos proxies, já que analisam e eventualmente filtram/bloqueiam conexões para determinados serviços. Porém, este elemento de segurança não intermedia as conexões, apenas aplicando regras de filtragem baseadas no conteúdo dos pacotes.

Comparando-o com os *firewalls* tradicionais, os *firewalls* de aplicações diferem no objeto da análise, incorporando o nível de filtragem de cabeçalho (endereçamento e portas de origem e destino), adicionadas da análise do nível da camada de aplicação (conteúdo dos pacotes).

Análise de Performance

A filtragem de pacotes tradicional, em termos de velocidade de repasse de pacotes, é entre 3 e 10 vezes mais veloz que a utilização de proxies de aplicação [1]. Este retardo é decorrente da filtragem de pacotes no nível de aplicação, característica dos proxies não presente nos *firewalls* tradicionais.

Na filtragem de aplicações, este retardo pode ser ainda maior, já que a análise e comparação dos dados dos pacotes em trânsito com padrões pré-estabelecidos (assinaturas) representarão, neste caso, um maior volume de utilização de recursos de processamento e memória da máquina.

O uso da filtragem em nível de aplicação na mesma máquina em que é realizada a filtragem de pacotes é desaconselhada em função do possível comprometimento de todo o processo de filtragem em decorrência do nível de análise dos pacotes resultando em degradação da performance [3] do *hardware* do *firewall*.

A análise dos dados (camada de aplicação) dos pacotes, portanto, tende a tornar-se inviável com o aumento do volume de informações que passam pelo filtro de aplicações se esta filtragem é feita na mesma máquina em que é realizada a filtragem de pacotes.

III. Sub-Rede de Filtragens Específicas (SuRFE)

A solução para esta situação é manter no *firewall* principal somente a filtragem de pacotes, desviando os pacotes endereçados a máquinas e/ou serviços internos específicos (análise baseada nas informações de endereço IP e porta de destino) para uma sub-rede de filtragem de aplicações. Nesta sub-rede, então, será realizada a filtragem na específica, bloqueando pacotes notadamente maliciosos, isto é, pacotes cujo conteúdo coincida com *strings* listadas na base de assinaturas de ataques carregadas pelo(s) *firewall(s)* de aplicações, conforme ilustrado nas Figuras 3 e 4.

A arquitetura desta sub-rede pode variar, conforme necessidades e/ou disponibilidades de recursos específicos. A seguir são apresentados os modelos básicos destas arquiteturas. A pesquisa em andamento consiste em implementar e determinar os impactos de utilização de cada um destes modelos, analisando a performance de roteamento e eficiência dos mecanismos de filtragem.

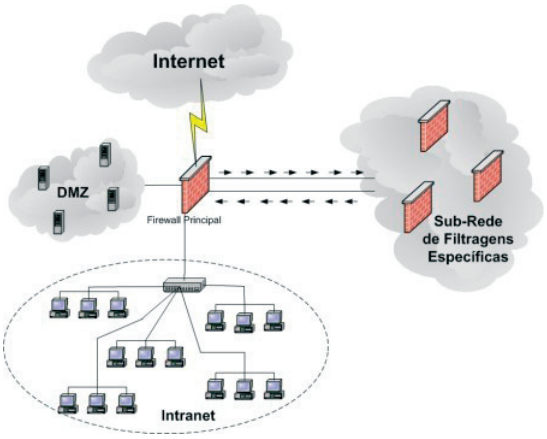


Fig. 3. Sub-Rede de Filtragens Específicas

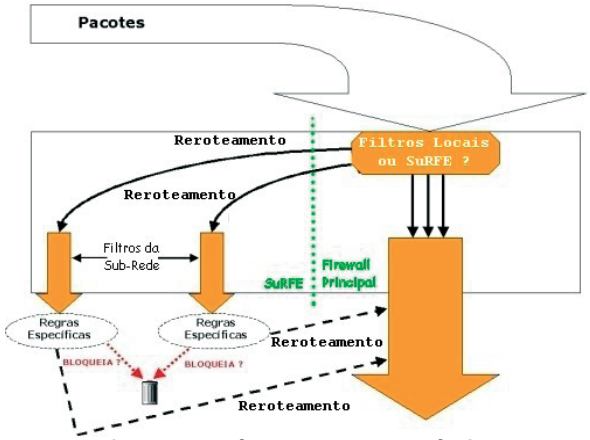


Fig. 4. Esquema de Funcionamento da SuRFE

A. Modelos Propostos

1) SuRFE com uma única máquina

Este é o modelo (Figura 5) de mais fácil implementação e de menor custo, já que envolve somente uma máquina adicional à estrutura pré-existente, e duas placas de rede no *firewall* para o desvio dos pacotes que serão analisados e retorno dos pacotes que não foram bloqueados pelas regras de filtragem. Entretanto, a utilização do re-roteamento deve ser um recurso suportado e implementado no firewall principal, já que somente os pacotes que se deseja analisar serão re-roteados para o filtro de aplicações (desvio baseado no serviço e/ou rede de origem/destino), sem modificação do cabeçalho, enquanto os demais pacotes serão filtrados e/ou repassados para seus destinos sem o re-roteamento.

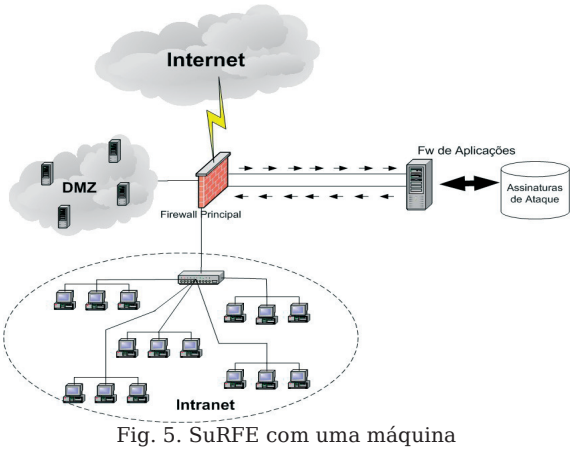


Fig. 5. SuRFE com uma máquina

2) SuRFE com Balanceamento de Carga

Neste modelo (Figura 6) será realizado o balanceamento de carga entre os firewalls da SuRFE (máquinas com o mesmo perfil) oferecendo redundância (alta disponibilidade) e escalabilidade para a solução.

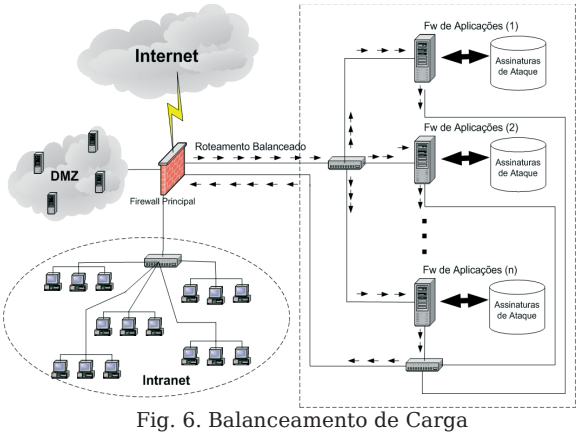


Fig. 6. Balanceamento de Carga

3) SuRFE com Separação por Aplicação

Neste modelo (Figura 7) a sub-rede de filtragem de aplicação é formada por *firewalls* com bases de assinaturas específicas para cada aplicação (porta ou conjunto de portas). O *firewall* principal redireciona os pacotes ao *firewall* de aplicação específico, de acordo com a aplicação destino de cada um deles.

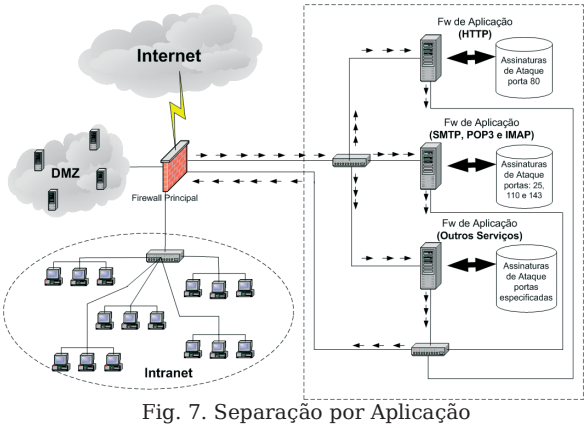


Fig. 7. Separação por Aplicação

IV. Conclusão

A insegurança das redes de computadores diante dos novos tipos de ataque que surgem a todo momento demanda soluções nem sempre satisfatórias do ponto de vista da usabilidade. Tornar um sistema minimamente seguro depende de decisões que podem resultar em problemas de indisponibilidade e até inviabilidade de determinadas aplicações cujo desempenho varia de acordo com o tempo de resposta.

O estudo de soluções de implementação simples que minimizem os impactos dos mecanismos de filtragem é uma necessidade tão crítica quanto as próprias soluções.

O objetivo final do estudo parcialmente detalhado neste artigo busca ratificar a viabilidade dos novos elementos de filtragem, minimizando o impacto de sua implementação pelo o tratamento específico de cada tipo de tráfego com a seleção adequada dos filtros a que serão submetidos.

References

[1] CHUVAKIN, Anton, *IPTables Linux firewall with packet string-matching support*: SecurityFocus , 2001.
[2] HUMES, Jeff. *Filtering packets based on string matching:* LinuxGuru.net, 2001.
[3] SILVA, Artur e PEIXOTO, Jarbas. *Iptables: Uma solução de baixo custo para implementação de firewalls p.102*: São Paulo.GTS, 2003.
[4] GONÇALVES, M. Firewalls – Guia Completo. Rio de Janeiro: Ed. Ciência Moderna, 2000.
[5] HATCH, B., LEE, J., KURTZ, G. Hackers Expostos – Linux. São Paulo: Makron Books, 2002.
[6] MARCIO, A Internet e os Hackers – Ataques e Defesas.São Paulo: Chantal, 2000.

Major Initiatives for Prevention and Mitigation of Cyber Crime in India: An Over View

Gulshan Rai and B Vasanta

Abstract—**The emergent information society is predicated on a sound platform of information and communications technology and especially anchored on the critical role of the Internet both as a tool and as a platform for delivering various e-services such as e-commerce, e-banking and e-governance amongst many others. With an increasing usage of Internet, and Cyber space offering a plethora of opportunities for criminals, the ICT industry and the society at large are facing serious challenges related to security and forensic issues. This paper presents major initiatives taken by Department of Information Technology, Government of India for prevention and mitigation of Cyber Crime in India. It also covers briefly some of the infrastructure and training programs of other Government Departments as well as major IT Industry Associations, in the area of cyber crime and forensics.**

Index Terms— **Cyber Crime, Cyber Forensics, Cyber Laws, Information Technology Act 2000.**

I. INTRODUCTION

As the Cyber Landscape is changing with technological changes in computers, networks and applications, so is the crime scene changing rapidly both within and outside the nations and has made a significant impact on the criminal justice system prevalent throughout the world. Its effects are felt more as nations constantly endeavor to provide quicker and more efficient services to its citizens through the use of cyber space. Globally not only the cyber landscape and hence the crime scene is changing but unfortunately the crime rate is increasing alarmingly both in value terms as well as in numbers. Each nation having different geographic, socio-economic and political structure is evolving its own strategies to tackle this issue.

India enjoys a competitive edge over many other neighboring nations particularly in the global ICT and software business in spite of its wide geographic, cultural and linguistic spread. It is known for its large pool of technical/ skilled human resource (English speaking). The Indian software industry is focusing on a robust Information Security environment which is essential in the cyber arena to maintain its competitive market position. However crime cannot be avoided and the cyber crime is even increasing as the usage of internet applications in the society is increasing. Prevention and mitigation of cyber crime therefore becomes an important issue. Major initiatives (in the civilian sector) taken by Government of India as well as industry to prevent and mitigate cyber crime, different aspects of which are handled by different organizations, are presented in this paper.

Ministry of Home Affairs, under the Central Government is the nodal ministry for managing law and order and internal security besides other activities. The Police, Bureau of Police Research & Development (BPR&D), National Crime Records Bureau (NCRB), Directorate of Forensic Science (DFS), National Police Academy (NPA) etc. are all under this Ministry. However the law and order at state level, is a state issue and each state has its own set up i.e. State Police, State Forensic Laboratories, and State Police Academies etc.

The Central Bureau of Investigation (CBI), functioning under Ministry of Personnel, Pension and Public Grievances, Government of India, is the premier investigating police agency in India, playing a major role as a national investigative agency. It is also the nodal police agency in India, which coordinates investigation on behalf of Interpol Member countries.

While the basic crime investigation responsibility as well as training its personnel lies with the Law enforcement agencies, the Department of Information Technology (DIT) being the nodal agency for Information Technology facilitates and strengthens their capabilities in handling the Technology crimes like cyber crimes. With a broad vision "To make India an IT Super Power by the Year 2008", DIT assumes the role of a

- Pro-active facilitator
- Pro-active motivator
- Pro-active promoter
- Spread of IT to masses and
- Ensure speedy IT led development

Gulshan Rai is with the Department of Information Technology, Government of India, New Delhi-110003, India. He is presently the Head of Cyber Laws Division and Director, CERT-IN.

B Vasanta, is Scientist F in the Department of Information Technology, Government of India, New Delhi-110003, India.(phone: 91-11-24363648, email: vasanta@mit.gov.in)

II. LEGAL FRAMEWORK

A. *Information Technology Act 2000*

As a first step to handle cyber crime, DIT has established a legal framework in India through enactment of the Information Technology (IT) Act 2000 by the Parliament. The Act provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "Electronic Commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies.

The Act defines various computer and crime related terms, offences as well as penalties and adjudication in such cases. The Act also provides for (i) appointing Adjudicating Officers to consider the cases of certain types of computer crimes in an expedite manner and (ii) establishing one or more appellate tribunals to be known as the Cyber Appellate Tribunal for considering the appeals arising out of the cases filed with Adjudicating Officers.

Government of India has notified the State Secretaries of IT departments as Adjudicating Officers.

As per the provision in the Information Technology Act 2000, the Cyber Appellate Tribunal consists of only one person, "The Presiding Officer of the Cyber Appellate Tribunal", who could be a judge of a High Court or a member of the Indian Legal Service and holding or has held the post of Grade I of that service for at least three years.

Recent developments nationally, and internationally particularly with respect to provisions related to data protection and privacy in the context of BPO operations, liabilities of network service providers, regulation of cyber cafes, new crimes etc. has brought the IT Act 2000 into focus again. With an objective to review the IT Act 2000, in the light of such developments and to consider the feedback received for removal of certain deficiencies in the Act, an Expert Committee was set-up. The Expert Committee has completed its deliberations and submitted its report giving due consideration for two main issues namely, (i) using the IT as a tool for socio-economic development and employment generation, and (ii) further consolidation of India's position as a major global player in IT sector. The Bill for amendment of IT Act 2000 is under process.

B. *Controller of Certifying Authorities*

The IT Act provides for setting up of the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities (CAs) who in turn issue digital signature certificates to users for electronic authentication.

The CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA. For this purpose it operates as the Root Certifying Authority of India (RCAI). The CCA also maintains the National Repository of Digital Certificates (NRDC), which contains all the certificates issued by all the CAs in the country.

The following are the licensed CAs in India:

1. SAFESCRIPT
2. National Informatics Center (NIC)
3. Institute for Development and Research in Banking Technology (IDRBT)
4. Tata Consultancy Services (TCS)
5. Mahanagar Telephone Nigam Limited (MTNL)
6. Customs & Central Excise
7. (n)Code Solutions

To generate awareness of the IT Act and its implementation, cyber crime & forensics etc, CCA also conducts seminars periodically.

C. *CERT-In*

The Indian Computer Emergency Response Team, CERT-In has been set up recently by DIT, to become the nation's most trusted referral agency for responding to computer security incidents as and when they occur; the CERT-In also assists members of the Indian Community in implementing proactive measures to reduce the risks of computer security incidents.

Besides providing a platform for incidence reporting, issuing virus alerts, advisories, vulnerability and incidence notes etc, CERT-In also publishes a monthly security bulletin and organizes workshops on related subjects.

CERT-In also empanels 'IT Security Auditors', for auditing, including vulnerability assessment and penetration testing of computer systems & networks of various Government organizations, the critical infrastructure organizations and those in other sectors of Indian economy.

III. CYBER CRIMES IN INDIA

NCRB publishes an annual report, "Crime in India" which is a compendium of crime statistics provided by the State Governments and Union Territories (UT) administrations and Heads of other Law Enforcement Agencies relating to Indian Penal Code (IPC) and other special and local laws portraying the overall crime scenario of the country in its various aspects. After the enactment of IT Act 2000 which has specified certain Computer, Network and Data related acts as punishable, Cyber Crime has found an entry into this Report. NCRB published data is used in this section.

During the year 2005, 179 cyber crime cases have been registered under IT Act 2000 as compared to 68 cases during

the previous year, as can be seen from Table 1 below, thereby reporting a significant increase of 163.2 percent in 2005 over 2004.

TABLE 1

CYBER CRIMES/CASES REGISTERED UNDER IT ACT 2000 DURING 2004-2005

S.No.	Crime Heads	Cases Registered 2004	2005
1.	Tampering (*Sec.65*)	2	10
2.	Hacking{*Sec.66(1), Sec.66(2)*}	26	74
3.	Obscene publication/transmission (*Sec.67*)	34	88
4.	Failure(*Sec.68, Sec.69*)	0	1
5.	Un-authorized access/attempt (*Sec.70*)	0	0
6.	Obtaining License or Digital Signature by misrepresentation/suppression of fact (*Sec.71*)	0	0
7.	Publishing false digital Signature certificate (*Sec.73*)	0	0
8.	Fraud – Digital Signature (*Sec.74*)	0	1
9.	Breach of confidentiality/privacy (*Sec.72*)	6	5
	Total:	**68**	**179**

Of the total 179 cases registered under IT Act 2000, about 50 percent (88 cases) were related to Obscene Publications / Transmission in electronic form, normally known as cyber pornography.

A. Crime, head-wise and age-group wise

TABLE 2

PERSONS ARRESTED UNDER CYBER CRIME, BY AGE GROUP, DURING 2005 (Offences Under IT Act)

S.No.	Crime Head	Below 18 yrs	Between 18-30 yrs	Between 30-45 yrs	Between 45-60 yrs	Above 60 yrs	Total
1.	Tampering	1	9	0	0	0	10
2.	Hacking						
	i)Loss/damage to computer resource	0	19	6	2	0	27
	ii)Hacking	0	12	2	0	0	14
3.	Obscence publication/transmission in electronic form	0	85	36	3	1	125
4.	Fraud Digital/ Signature	0	0	3	0	0	3
5.	Breach of confidentiality/ privacy	0	6	6	1	0	13
	Total:	**1**	**131**	**53**	**6**	**1**	**192**

Profile of the offenders arrested under IT Act 2000 is shown in Table 2 above. The age-wise profile of persons arrested in Cyber Crime cases under IT Act, 2000 shows that 68.2 percent of the offenders were in the age group 18 – 30 years (131 out of 192) and 27.6 percent of the offenders were in the age group 30- 45 years (53 out of 192). Nearly 65.1 percent (125 out of 192) of the offenders were arrested under head 'Obscene publication/transmission in electronic form' of which 68.0 percent (85 out of 125) were in the age-group 18 –30 years. Of the total persons arrested for 'Hacking Computer Systems', more than 75 percent (31 out of 41) were in the age group of 18-30 years.

The data clearly indicates that persons in the age group 18-30 years commit cyber crimes more, and obscene publication/transmission in electronic form is the most common cyber crime committed during the year 2005.

B. Incidence of Cyber Crimes in Cities

From the cyber crime data as reported in the NCRB report, it has also been found that 25 cities out of 35 mega cities in India (with population of more than 1 million) did not report any case of Cyber Crime during the year 2005. The cyber crimes are registered either under the IT Act 2000 or under IPC. The cases reported under IPC are shown in Table3 below.

TABLE 3

INCIDENCE OF CYBER CRIME CASES REGISTERED IN MEGA CITIES DURING 2005 (OFFENCES UNDER IPC)

S.No	City	Forgery	Breach of Trust Fraud	Currency Stamp Paper Fraud	Total
1.	Ahmedabad	2	5	-	7
2.	Delhi	8	-	-	8
3.	Meerut	-	1	-	1
4.	Surat	2	113	31	146
5.	Vijayawada	1	-	-	1
	TOTAL	**13**	**119**	**31**	**163**

Non reporting of cases under the IT Act 2000, from some of the mega cities could be partly due to fear of losing reputation/brand name on the part of the victims and partly due to insufficient understanding and interpretation of different Sections of IT Act 2000 on the part of Law Enforcement Personnel or other reasons which may need further analysis. The high incidence of crime, for example in Surat could be a random incidence in 2005 but needs further studies as well as more statistically dependable data to draw any conclusion.

Only 5 mega cities have reported 163 cyber crime cases

under IPC. There has been a significant increase of 527 percent (from 26 cases in 2004 to 163 cases in 2005) in cases as compared to previous year (2004). While increasing population is observed to be one of the important factors influencing incidence of crime, increased criminal activities in mega cities could also be on account of unchecked migration, socio-cultural disparities, uneven distribution of incomes etc. More data and detailed analysis are required to correlate these statements.

IV. INFRASTRUCTURE FACILITIES

The Directorate of Forensic Science under the Ministry of Home Affairs, with its three Computer Forensic Labs (CFLs) and three offices of Government Examiner of Questioned Documents (GEQDs) provides the necessary forensic analysis expertise to the Law enforcement agencies. Most of the States also have Forensic Science Laboratories, and some of the cyber crime cells at the state police stations also have limited facilities and expertise to handle common cyber crimes related to emails, pornography, hacking etc. However, the Central and State Forensic Laboratories are more conversant with conventional areas of forensics like Ballistics, Toxicology/Serology, Physical & Chemical sciences etc. and Computer/Cyber forensics has not yet been identified as an independent discipline in forensics. Cyber forensics is one amongst many other crime investigation facilities operated by these organizations and being a new area, have scanty infrastructure & trained personnel. Very few of them have facilities and expertise to meet the changing needs in cyber crime investigations.

Two technical resource centers, one focusing on computer disk forensics and the other on steganograhy, set up at Center for Development of Advanced Computing (CDAC) Thiruvananthapuram and Kolkata respectively, have been sponsored by DIT. These centers besides research also facilitate law enforcement agencies in cyber crime investigations.

V. TRAINING

For successful prosecution of cyber crimes it is essential to have adequate and cogent digital evidence against the suspect and then link this information to the suspect in a legally acceptable manner. Information stored in digital form is transient in nature and therefore law enforcement personnel require specialized skills to seize, collect, analyze and report digital evidence in a Court of Law.

Many organizations like NCRB-Delhi, CBI Academy-Ghaziabad, National Police Academy -Hyderabad etc conduct training programs, generally on computers software packages and fundamentals of cyber forensics. Some collaborative training programs with FBI are also conducted. CERT-IN, CCA, CFSL etc conduct some subject specific courses on Cyber Security, Cyber Laws, Cyber Crimes & related issues. In general, the courses on cyber forensic tools, their suitability for specific applications, comparisons, technology & crime trends, international best practices etc are rare or very few. Police personnel are also frequently transferred to hold different assignments & hence there is a continuous need for training in the enforcement department. Also, as most of the crimes involve use of computers & electronic gadgets at some stage of committing the crime or the other, basic knowledge & training in digital evidence is always desirable and advantageous for the law enforcement personnel. There is an urgent need for conducting more training programs and there is scope for public private partnership as well as international cooperation in this area.

VI. INTERNATIONAL COOPERATION

Cyber Crime cases are covered under Mutual Legal Assistance Treaties (MLATs), which India has with various countries. Moreover, India is a member of Cyber Crime Technology Information Network System (CTINS), which is a Japanese Govt. initiative for mutual exchange of information regarding cyber crimes among the member countries, which is advisory in nature. This system is presently installed in the Cyber Crime Investigation Cell of Central Bureau of investigations (CBI), which is also 24x7 point of contact for Sub Group of Hi-tech Crimes of G-8 Countries.

VII. INDUSTRY INITIATIVES

The two industry associations in India which are participating in major promotional activities in the IT sector are, National Association of Software and Service Companies, NASSCOM, and Manufacturer Association of Information Technology, MAIT.

MAIT, initially set up for purposes of scientific, educational and IT industry promotion, has emerged as an effective and dynamic organization with majority of the Members coming from the Hardware Sector, by turnover, and the remaining from Training, Design, R&D and the associated services sectors of the Indian IT Industry. MAIT's charter is to develop a globally competitive Indian IT Industry, promote the usage of IT in India, strengthen the role of IT in national economic development and promote business through international alliances. The organization's special focus is on domestic market development and attracting foreign investment in the Indian IT Industry.

NASSCOM, the premier trade body and the chamber of commerce of the IT software and services industry in India was set up to facilitate business and trade in software and services and to encourage advancement of research in software technology. It is a not-for-profit organization. With over 1050 members, of which over 150 are global companies from the US, UK, EU, JAPAN AND CHINA, NASSCOM is a true

global trade body, with member companies in the business of software development, software services, software products and it-enabled/bpo services.

Information Security remains one of the key priorities for the Indian IT Enabled Services –Business Process Outsourcing (ITES-BPO) industry, a challenge that has to be overcome in order to firmly establish the sector's credentials as a trusted sourcing destination. Recognizing the fact that security breaches in leading BPO firms can put a spanner in India's successful outsourcing run, the industry has come forward to devise roadmaps and outline strategies that will help create an impregnable Information Security environment. The country, in fact has been working very closely with representatives of the US market, the largest outsourcer of processes to India. Two years ago, this collaborative effort bore fruit as the Indian IT-ITES industry, represented by NASSCOM and the US market, represented by the Information Technology Association of America (ITAA), came together to launch the prestigious "India-US Information Security Summit."

Cyber laws, cyber security, cyber crime etc are important issues discussed in several seminars and workshops conducted periodically by the industry associations.

A joint initiative of NASSCOM and Mumbai Police, the Mumbai Cyber Lab is a unique initiative of Police-Public collaboration to facilitate investigations of cyber crime; some of its the broad objectives are to:

- Promote collaboration among Mumbai Police, Information Technology industry, academia and concerned citizens to address cyber crime and its related issues.
- Develop pro-active strategies for anticipating trends in cyber crime and formulating technical and legal responses on various fronts.
- Facilitate cyber crime investigation training among police officers.
- Develop cyber crime technology tools for criminal investigation. Improve awareness of cyber crime among the people and enhance Information Security in Mumbai city in general.
- Act as Resource Center for other police organizations in the country.

VIII. CONCLUSION

To combat cyber crime, India, besides ensuring a robust Information Security environment, has put up a legal framework in place, initiated awareness and training programs and set up cyber forensic facilities. However the cyber crime data for year 2005 indicates an increase in the crime rate, particularly in mega cities and more offenders are in the age group, 18-30 years which draws special attention and needs further studies to understand the motives, implications etc. More focused awareness and training programs in cyber crime related topics and social engineering in general and for this age group in particular involving private partnership could probably go a long way in improving the scenario.

Acknowledgment

The authors wish to acknowledge making extensive use of information available in public domain from the reference sites given below for preparing this paper.

NOTE: The views expressed in this paper are those of the authors and do not reflect those of Government of India.

REFERENCE SITES/PAGES

http://www.mit.gov.in/it-bill.asp

http://www.cca.gov.in/index.jsp

http://www.cert-in.org.in/roles.htm

http://mha.nic.in/police_main.htm

http://ncrb.nic.in/crime2005/home.htm

http://www.nasscom.in/Nasscom/templates/NormalPage.aspx?id=11154

http://www.mumbaicyberlab.org/about/vision.htm

http://www.mait.com/aboutus.htm

NOTAS

NOTAS

REALIZAÇÃO

9 771980 111000