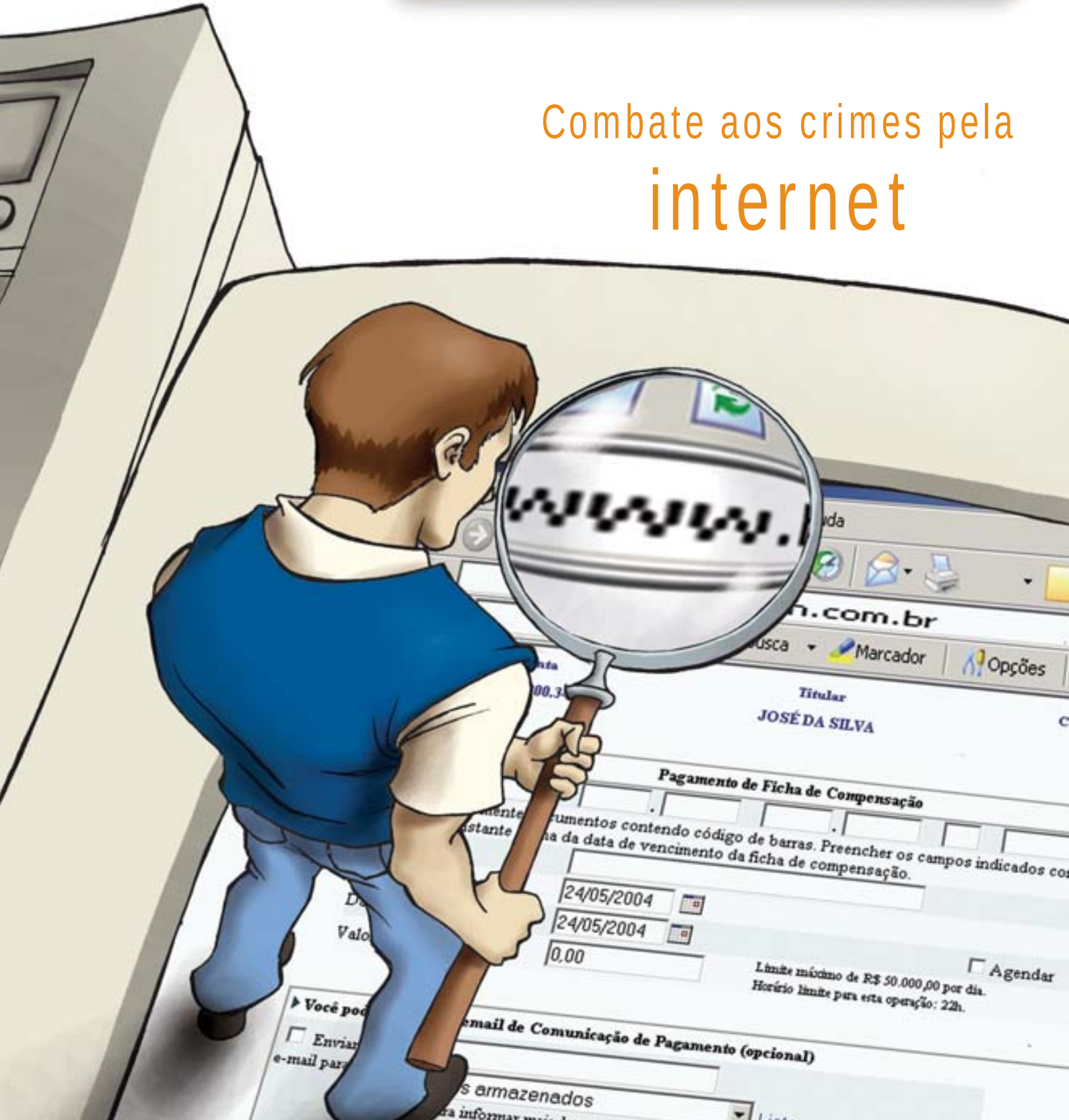
ENTREVISTA
Sérgio Amadeu
PÁGINAS 4 A 5

APCF
Associação Nacional dos Peritos Criminais Federais

PERÍCIA FEDERAL

Distribuição Gratuíta
Ano V – Número 17 – janeiro a junho de 2004

Combate aos crimes pela internet



Diretoria da Executiva Nacional

Roosevelt A. F. Leadebal Júnior Presidente	Eurico Monteiro Montenegro Suplente de Secretário Geral	Renato Rodrigues Barbosa Diretor Financeiro	Luiz Eduardo Lucena Gurgel Suplente de Diretor de Comunicação
Antônio Carlos Mesquita Vice-Presidente	Jorilson da Silva Rodrigues Diretor Jurídico	Eduardo Siqueira Costa Neto Suplente de Diretor Financeiro	Dulce Maria P. Santana Diretora Técnico-Social
Bruno Costa Pitanga Maia Secretário Geral	Luiz Carlos de G. Horta Suplente de Diretor Jurídico	Paulo Roberto Fagundes Diretor de Comunicação	Marcos de Almeida Camargo Suplente de Diretor Técnico-Social

Conselho Fiscal Deliberativo (O Conselho Fiscal Deliberativo é formado por cinco peritos, três titulares e dois suplentes)

Carlos Maurício de Abreu - DF Titular	José Gomes da Silva - DF Titular	Emanuel Renan C. Coelho - DF Titular	Paulo Ricardo Manfrin- SC Suplente	Gutemberg de A. Silva - BA Suplente

Diretorias Regionais

ACRE
Diretor: Alexandro Mangueira Lima de Assis
Suplente: Flávia Freitas de Siqueira
apcf.ac@apcf.org.br

ALAGOAS
Diretor: Nivaldo do Nascimento
Suplente: Murilo Castelões de Almeida
apcf.al@apcf.org.br

AMAZONAS
Diretor: Fernanda Scarton Kantorsky
Suplente: Antônio Carlos de Oliveira
apcf.am@apcf.org.br

BAHIA
Diretor: José Carlos de Souza Ferreira
Suplente: Iracema Gonçalves de Alencar
apcf.ba@apcf.org.br

CEARÁ
Diretor: João Vasconcelos de Andrade
Suplente: Maria Marta Vieira de Melo Lima
apcf.ce@apcf.org.br

DISTRITO FEDERAL
Diretor: André Luiz da Costa Morisson
Suplente: Charles Rodrigues Valente
apcf.df@apcf.org.br

ESPÍRITO SANTO
Diretor: Roberto Silveira
Suplente: Paulo dos Santos
apcf.es@apcf.org.br

GOIÁS
Diretor: Luiz Pedro de Sousa
Suplente: Francisco William Lopes Caldas
apcf.go@apcf.org.br

MARANHÃO
Diretor: Eufrásio Bezerra de Sousa Filho
Suplente: Luiz Carlos Cardoso Filho
apcf.ma@apcf.org.br

MATO GROSSO
Diretor: Waldemir Leal da Silva
Suplente: Ruy César Alves
apcf.mt@apcf.org.br

MATO GROSSO DO SUL
Diretor: André Luis de Abreu Moreira
Suplente: Everaldo Gomes Parangaba
apcf.ms@apcf.org.br

MINAS GERAIS
Diretor: João Luiz Moreira de Oliveira
Suplente: Lúcio Pinto Moreira
apcf.mg@apcf.org.br

PARÁ
Diretor: Antonio Carlos F. dos Santos
Suplente: João Augusto Brito de Oliveira
apcf.pa@apcf.org.br

PARAÍBA
Diretor: Antônio Vieira de Oliveira
Suplente: Maria Irene de S. Cardoso Lima
apcf.pb@apcf.org.br

PARANÁ
Diretor: Fabiano Linhares Frehse
Suplente: Magda Aparecida de A. Kemetz
apcf.pr@apcf.org.br

PERNAMBUCO
Diretor: Rinaldo José Prado Santos
Suplente: Maria da Penha N. de Aguiar
apcf.pe@apcf.org.br

PIAUÍ
Diretor: José Arthur de Vasconselos Neto
Suplente: Henrique Santana da Costa
apcf.pi@apcf.org.br

RIO DE JANEIRO
Diretor: Isaque Morais da Silva
Suplente: Délglen Jeane Bispo
apcf.rj@apcf.org.br

RIO GRANDE DO NORTE
Diretor: Débora Gomes de M. Santos
Suplente: Elinaldo Cavalcante da Silva
apcf.rn@apcf.org.br

RIO GRANDE DO SUL
Diretor: Dirceu Emílio de Souza
Suplente: Marcelo de Azambuja Fortes
apcf.rs@apcf.org.br

RONDÔNIA
Diretor: Abílio Jorge Leitão Felisberto
Suplente: Odair de Souza Glória Júnior
apcf.ro@apcf.org.br

SANTA CATARINA
Diretor: Maria Elisa Bezerra de Souza
Suplente: Athos Cabeda Faria
apcf.sc@apcf.org.br

SÃO PAULO
Diretor: Eduardo Agra de Brito Neves
Suplente: Sérgio Barbosa Medeiros
apcf.sp@apcf.org.br

SERGIPE
Diretor: Reinaldo do Couto Passos
Suplente: César de Macêdo Rêgo
apcf.se@apcf.org.br

TOCANTINS
Diretor: Evaldo Oliveira de Assis
Suplente: Élvio Dias Botelho
apcf.to@apcf.org.br

Expediente

Planejamento e produção: Oficina da Palavra Ltda- fone 322-6753/6754
oficina@oficinadapalavra.com
Edição: Anelise Borges
Arte: Cícero e Gabriela Pires

Diagramação: Varilandes Júnior
Capa: Amauri Ploteixa e Cícero
Tiragem: 3.000 exemplares
A revista Perícia Federal é uma publicação quadrimestral da APCF. A revista não se responsabiliza por informes publicitários nem por opiniões e conceitos emitidos em artigos assinados
As correspondências poderão ser enviadas para: Revista Perícia Federal: SEPS 714/914 Centro Executivo Sabin, bloco D, salas 223/224 CEP 72390-145 - Brasília/DF
Telefones: (61) 346-9481/345-0882
e-mail: apcf@apcf.org.br
www.apcf.org.br

SUMÁRIO

EDITORIAL

É chegada a hora da mudança

Desde meus tempos de estudante de economia reflito sobre a importante distinção proposta pelo austríaco Joseph A. Shumpeter (1883-1950), em sua obra "Teoria do Desenvolvimento Econômico" (várias edições), entre o verdadeiro "desenvolvimento" e a mera "mudança", coisas tão diferentes, dizia ele, quanto "abrir uma nova estrada e caminhar por ela".

Arquivo APCF

> **"Não adianta empilhar inquéritos em um himalaia de papel se o perito continua privado de meios materiais, tecnológicos e organizacionais para combater a impunidade"**

Se esse discernimento fosse seriamente aplicado à área da segurança pública, perceberíamos que as propostas de mudança, que se multiplicam na proporção da escalada dos índices de violência, criminalidade e impunidade, em sua maioria pouco contribuem para desenvolver as organizações policiais e capacitá-las a conter e inverter essa tendência.

No dia-a-dia, a inércia da rotina arrasta as autoridades para o beco sem saída do "mais do mesmo": contratar mais policiais, comprar mais viaturas, mais armamentos. Ora, ninguém produz resultados novos porfiando em velhos métodos. E, segundo Shumpeter, o desenvolvimento surge apenas quando o novo aparece. Um exemplo de ação nova, que promoveria um salto de qualidade nas investigações policiais, é o reconhecimento constitucional da produção da prova pericial como atividade-fim das polícias. Não adianta empilhar inquéritos abertos pelo delegado em um himalaia de papel se o perito continua privado de meios materiais, tecnológicos e organizacionais suficientes para provar quem são os culpados, de forma rápida e definitiva, e assim combater a impunidade. Para criar raízes e dar frutos, esse novo conceito precisa começar a ser cultivado nas academias de polícia, o que, por sua vez, exigirá uma reforma curricular corajosa.

Shumpeter enfatiza que o motor do desenvolvimento é a figura do empreendedor, dotado de energia e liderança para enxergar o novo, compartilhar sua visão com os colaboradores e mobilizá-los para a ação. O setor de segurança pública anda carente de autoridades que tenham coragem de assumir riscos e implantar idéias novas; de questionar estruturas, rotinas, hábitos mentais consolidados; de enfrentar os interesses corporativos sempre que estes contradizem as necessidades coletivas.

Em tempos tão difíceis como o vivido nesta greve, esta reflexão também se estende ao movimento classista. O novo tem que chegar e atuar como catalisador dessa revolução empreendedora formulando análises críticas, com ética, veiculando diagnósticos verdadeiros, abraçando idéias, reivindicações e propostas que possam desenvolver a segurança pública e retirá-la do atual estado de "falência múltipla" dos seus órgãos, sob pena de ficar preso ao passado e sucumbir perante os novos anseios sociais. ■

Tecnologia da Informação: a serviço da segurança pública

Divulgação

Sérgio Amadeu, presidente do Instituto de Tecnologia da Informação (ITI), é sociólogo e mestre em Ciência Política pela Universidade de São Paulo. Sua tese de mestrado tratou do Poder no Ciberespaço, o controle e regulamentação da internet. Sérgio Amadeu é ainda doutorando pela USP, onde estuda a teoria democrática na era da informação.

Com um trabalho extenso na área de internet, ele foi o responsável pela implantação do governo eletrônico da prefeitura de São Paulo. Também executou o plano de inclusão digital da cidade de São Paulo. Integrou o Comitê Gestor da internet brasileira que formulou o novo modelo de governança da rede no Brasil.

Amadeu é autor do livro Exclusão Digital: a Miséria na Era da Informação, editado pela Perseu Abramo. E ainda organizou a coletânea Software Livre e Inclusão Digital da Conrad Editora, sendo um dos seus autores.

Sérgio Amadeu é o entrevistado desta edição da Revisa Perícia Federal. Na entrevista, ele fala sobre o processo de certificação digital e de que forma este processo pode ser útil na área de segurança pública e em outras tantas áreas do governo federal.

Perícia Federal - O processo de obtenção de certificados digitais envolve a identificação de pessoas, momento em que são apresentados documentos de identidade e conferidas assinaturas manuscritas. Uma vez que existem esforços dirigidos para aprimorar os processos de identificação civil e criminal, seria este o momento para introduzir a identificação digital para o cidadão?

Sérgio Amadeu - O processo de identificação da ICP - Brasil para a pessoa que vai obter o certificado é muito rigoroso. Para isso existe uma autoridade de registro que tem que seguir regras, coletar documentos e tem que assegurar que o par de chaves criptográficas, emitidas pelo cidadão, seja de seu exclusivo controle. A AR não pode, em nenhum momento, ter uma cópia da chave privada do cidadão e não pode guardar isso em nenhuma de suas máquinas, portanto existe uma grande preocupação de um lado, que garante a segurança do processo, e do outro garante a privacidade do cidadão. A identidade digital é um processo mais complexo que passa por uma decisão política do governo. Sem dúvida nenhuma, se algum dia tivermos uma identidade digital, essa identidade será baseada em criptografia, provavelmente em criptografia assimétrica, portanto nós acreditamos que isso vá ocorrer algum dia, mas nossa preocupação hoje é ampliar a base da certificação digital. Vivemos ainda num país de excluídos digitais, apontando a importância de utilizar a certificação digital. Por exemplo, no imposto de renda de pessoas jurídicas: isso colocaria algo em torno de 5 milhões de certificados digitais e prontamente ajudaria a viabilizar o mercado de certificação digital no Brasil, popularizando seu uso.

Perícia Federal - Pretende-se substituir os atuais passaportes brasileiros por documentos mais seguros. Existe a possibilidade da certificação digital oferecer segurança adicional neste processo?

Sérgio Amadeu - Sim, existe. A certificação digital pode ser empregada em vários processos do governo, ampliando enormemente a segurança desses processos e diminuindo drasticamente as fraudes e as possibilidades de falsificação. Essa é uma decisão do Ministério de Justiça e da Polícia Federal. Nós e a infra-estrutura de chaves públicas e suas Acs, estamos em plenas condições de oferecer soluções imediatas para resolver essa questão. Quanto a questão da substituição do passaporte seria muito bom se as pessoas tivessem, ao invés do passaporte, um smart card e que dentro dele, num dos slots, que possivelmente nós poderíamos colocar, ter informações sobre os vistos e ,em um outro, ter o módulo criptográfico com as chaves privadas. Mas isso requer uma adoção pela Organização das Nações Unidas. Aliás, o Brasil poderia propor esse assunto, mas isso tem que ser muito estudado e vai existir sempre aquela grande questão colocada: como um país que construiu sua infra-estrutura de chaves públicas, com níveis de segurança discutíveis, muito inferiores, como aceitar esse passaporte? Esse smart card? Como é que vai ser esse processo?

Esse processo precisa ser elaborado, muito bem pensado e vai envolver, certamente, decisões complexas no terreno da política internacional.

Perícia Federal - A perícia possui uma linha de trabalho dirigida a comprovação da autenticidade de documentos, conhecida como Documentoscopia. Será que já se pensou em contar com seus profissionais para promover o uso da certificação digital, uma vez que eventualmente eles mesmos serão chamados para solucionar contenciosos que envolvam documentos eletrônicos?

Sérgio Amadeu - O ITI ajudou no processo de construção da política industrial que o Presidente Lula anunciou na área de software. Ele inseriu uma série de preocupações nesse conjunto de políticas relativas às empresas de segurança que trabalham na área de tecnologia da informação. Nós achamos que existe um enorme espaço para o desenvolvimento de soluções por empresas que podem ser empregadas na área de segurança pública, na área de planejamento de segurança e na área policial. É preciso que essas propostas sejam colocadas adiante principalmente pelas agências de financiamento (BNDES) para que essas empresas possam conversar com as universidades, que possuem muitos projetos bons que poderiam virar inovação, e inovação vira produto, então, eu acredito que isso faz parte da política de software, que está dentro da política industrial e vai ser colocado em prática.

É uma excelente idéia trabalhar a certificação digital integrando os diversos orgãos que tem especialidades afins. Nós já estamos fazendo isso com a Marinha, com CEPESC, com ABIN e acho fundamental incorporar esse departamento da Polícia Federal.

Perícia Federal - Sendo o senhor um sociólogo, como o Sr. vê o futuro da investigação criminal e o emprego de técnicas científicas para desvendar crimes?

Sérgio Amadeu - Do ponto de vista social, a tecnologia é nitidamente crescente e, cada vez mais, passa a dominar um conjunto enorme do cotidiano, seja da sociedade, dos governos ou das instituições. Por isso que eu costumo dizer que as sociedades são "tecnodependentes", elas sempre dependeram de um conjunto de tecnologias. As tecnologias vitais hoje são tecnologias da informação, então, sem dúvida nenhuma, os países que quiserem ter mais vantagens em solucionar crimes, em ter uma investigação mais precisa, em cometer um número menor de erros policiais e usar mais a inteligência, terão que recorrer a essas tecnologias que, aliás, são tecnologias da inteligência, então, sem dúvida alguma, a tendência é você ter um conjunto de soluções e de sistemas que facilitem mais ainda o trabalho daqueles que são os defensores da lei. De um lado isso gera uma maior eficiência na atividade judicial e policial, mas tem um inconveniente que precisa ser dito: nunca na humanidade nós tivemos tanta possibilidade de vigilância sobre os cidadãos, sobre o seu dia-a-dia. O Estado e a polícia também terão que se preocupar em como não realizar invasões desmedidas na vida das pessoas, para não transformá-las em prisioneiros digitais. Quando as pessoas navegam na rede, fazem suas compras no comércio eletrônico, freqüentam sites culturais ou de entretenimento, elas geram rastros digitais e nós não podemos permitir que esses rastros sejam usados de maneira imprópria. A tecnologia gera pontos positivos e negativos e é preciso saber muito bem quem vai decidir sobre como será o seu pleno uso. Não é uma questão técnica, isso são questões políticas e são questões que devem ser encaradas num fórum democrático.

> “A certificação digital pode ser empregada em vários processos do governo, ampliando enormemente a segurança desses processos e diminuindo drasticamente as fraudes e as possibilidades de falsificação”

Perícia Federal - Será que a justiça brasileira vai conseguir superar sua atração pelo papel com o uso massificado de documentos eletrônicos?

Sérgio Amadeu - Eu acredito que a justiça está avançando muito e possui várias experiências: tribunais inteiros são tribunais eletrônicos, e com a presidência atual do STJ do Ministro Vidigal, que é um profundo conhecedor de tecnologia da informação, tenho certeza que o Judiciário vai dar um salto em agilidade, em modernização e no uso da rede informacional.

Perícia Federal - Quais as perspectivas do Instituto de Tecnologia da Informação quanto à disseminação do uso de certificação digital no âmbito do governo?

Sérgio Amadeu - Nós estamos apostando muito em produzir um decreto com o Presidente da República, onde os principais sistemas estruturadores do governo federal sejam acessados pelos funcionários públicos a partir de certificados digitais. Isso vai permitir que o funcionário público tenha contato com essa importante tecnologia e que passe também a viabilizar os documentos eletrônicos pois, uma vez que ele tem o certificado digital, esse certificado não vai servir apenas para que ele acesse na verdade os sistemas que estão no Serpro, por exemplo, mas vai permitir que aquele mesmo certificado possa assinar um documento, que passa a ter validade jurídica. Então ele pode mandar um documento para o ministro assinar que recebeu de uma outra autoridade. Isso vai se disseminar pela Esplanada. Mas qual o começo de tudo? O começo de tudo é que é preciso um incentivo e o incentivo surge com uma data a partir do qual todos os funcionários tenham que usar certificado digital para acessar os sistemas. Nós sabemos que tentativas simplesmente de convencer, sem um uso claro, não vai permitir que a gente tenha essa popularização na Esplanada, então nós estamos trabalhando junto com a SLTI e o Serpro para poder tentar chegar a um acordo num bom texto que viabilize o fio da meada. Vamos dizer, a lição de casa do governo é fazer os funcionários públicos usarem os certificados digitais aumentando a segurança dos processos, a agilidade, diminuindo o número de papel e o tempo para deslocamento de processos. ■

Agentes Inteligentes Móveis
no Combate às Invasões Cibernéticas

"Já é hora de refletir e combater os novos tipos de crimes que surgem no mundo virtual"

"Para muitas pessoas, as redes de computadores representam uma nova era na comunicação humana. O anonimato na comunicação sugere que a rede de computadores é um lugar seguro e sem práticas ilícitas. Infelizmente, esse ponto de vista utópico não é realista"

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

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

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

Agentes

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

Características Esperadas dos Agentes

Alguns atributos que caracterizam os agentes no mundo cibernético são:

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

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

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

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

COLABORAÇÃO

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

Interação do agente com o ambiente

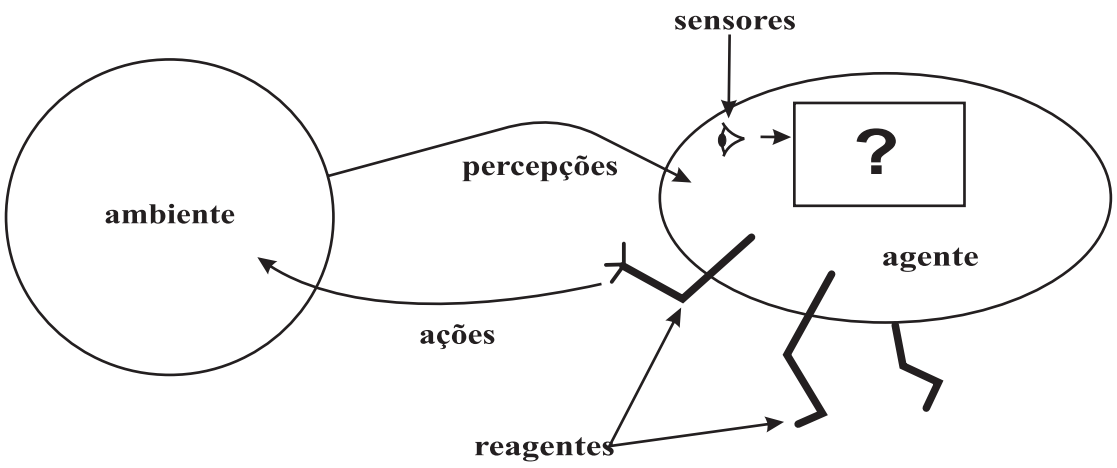


Figura 1

Aplicação Apropriada para Agentes

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

Segurança de redes

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

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

Acesso e Gerenciamento Móvel

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

Correio eletrônico e troca de mensagens

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

Colaboração

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

Interfaces inteligentes

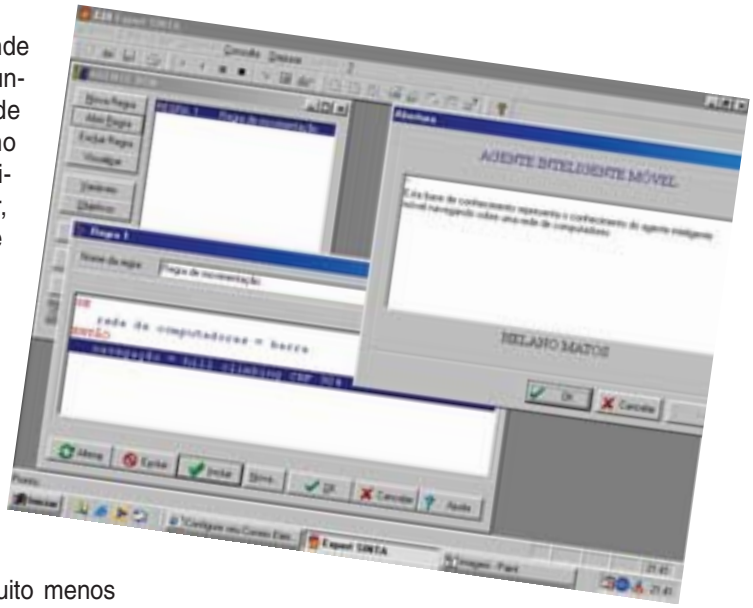
Apesar da disseminação de interfaces gráficas (GUI), para muitas pessoas, os computadores continuam difíceis de usar. Por outro lado, a medida em que a população de usuários cresce e se diversifica as interfaces se tornam mais e mais complexas para acomodar hábitos e preferências variadas. Agentes de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

Combate Cibernético

Como visto na seção anterior, a tecnologia de agentes pode resolver muitos problemas de diferentes formas. Em um primeiro momento aplicamos os agentes móveis para resolver o importuno problema dos ataques de negação de serviço (DoS ou DDoS) na transmissão em rede.

Na rede, a largura da banda é um fator importante e algumas vezes um raro recurso de aplicação distribuída. A transação solicitada entre um cliente e um servidor pode requerer muitas voltas sobre a rede para ser completada. Este tipo de operação cria um tráfego muito grande e consome muito da banda de transmissão.

Em um sistema sob ataque de hackers com muitos "clientes" e sistemas invadidos, o total de solicitações da banda pode exceder a disponibilidade permitida, ocasionando uma performance muito ruim para as aplicações que estão envolvidas ou mesmo a parada total do sistema, configurando uma invasão do tipo DoS. Com a utilização de agentes para buscar as solicitações ou transações, enviando os agentes do cliente para o servidor, o fluxo na rede é reduzido. Desta maneira, somente o que os agentes encontrarem será transmitido pela rede, tornando a velocidade de transmissão maior. A arquitetura de agente projetada toma decisões sobre onde uma parte da funcionalidade pode residir, baseado no número de solicitações ao servidor, na banda de transmissão, no tráfego na rede, no número de clientes e servidores, dentre outros fatores.



Arquiteturas baseadas em agentes móveis são potencialmente muito menos suscetíveis a problemas de flexibilidade de ambientação do programa computacional. Algumas decisões devem ser feitas para melhorar o tempo gasto com desenvolvimento e o sistema é mais fácil de ser modificado depois de ser construído. Essa proposta de arquitetura de agentes suporta adaptações da rede podendo fazer um novo desenho automaticamente. Este modelo de agentes também pode resolver problemas criados por intermitência ou má qualidade da conexão com a rede.

Atualmente algumas aplicações na rede são pesadíssimas para completar a transação ou obter localização de informação. Se, por exemplo, uma conexão cair, o cliente deve reiniciar a transação do ponto de partida. Com a tecnologia de agentes o cliente poderá obter as informações, mesmo que a conexão não esteja ativa, trabalhando off-line. Os agentes podem completar as transações e retornar os resultados para o cliente quando for restabelecida a conexão. Desta forma, a comunidade da inteligência artificial, tem lutado intensamente por mais de duas décadas e este potencial de aplicações é imensurável.

Conclusões e Tendências Futuras

Este trabalho apresenta um estudo de agentes que possuem mobilidade e comportamento inteligente. Ademais, foi desenvolvida uma arquitetura de agentes baseado em linguagem de programação PROLOG para realizar uma forma de monitoração e combate de invasões DoS e DDoS com o intuito de combatê-las de forma automática e sem necessitar a intervenção humana.

Todavia, é preciso melhorar a interface e ampliar o escopo de atuação do agente inteligente móvel implementado. Agora, predizer qual será o papel dos agentes no futuro e como eles serão construídos, não é uma tarefa fácil.

Entretanto, já existem várias aplicações baseadas em agentes que facilitam a vida dos usuários que usam redes de computadores, em destaque para internet. Grandes universidades, centros de pesquisa e um número considerável de companhias, como a IBM e Microsoft, estão fazendo pesquisas na área de agentes inteligentes e o Departamento de Polícia Federal não pode ficar aquém a esta nova tecnologia. ■

Entendendo e Utilizando a Internet com Segurança

Uma visão geral sobre segurança e vulnerabilidades nas comunicações via internet

Com a disseminação do uso da internet surgiram vários tipos de serviços na World Wide Web que exigem um alto nível de segurança nas comunicações, tais como transações bancárias, lojas virtuais, dentre outros. Nesses serviços, informações como números de cartões de crédito e senhas bancárias, por exemplo, não podem trafegar livremente sem nenhuma forma de proteção contra indivíduos mal intencionados. Diante desse cenário, preparamos este artigo com o intuito de fornecer uma visão geral sobre os mecanismos e recursos de segurança comumente disponíveis quando utilizamos serviços através da Internet.

Comunicações Seguras

Inicialmente, devemos compreender quais aspectos de segurança podem ser comprometidos em uma rede mundialmente interligada. Como o tráfego na internet passa por diversos computadores e dispositivos intermediários antes de chegar ao seu destino, um usuário mal intencionado pode comprometer a segurança dos dados em uma comunicação através das seguintes formas:

Escuta
Um usuário não autorizado pode visualizar e guardar todo o tráfego que passa por um determinado dispositivo da rede, sem alterá-lo;

Personificação
Alguém se faz passar por outra entidade, assumindo uma falsa identidade e ludibriando o outro participante em uma comunicação;

Adulteração
Informações são alteradas, acrescentadas ou removidas em uma comunicação.

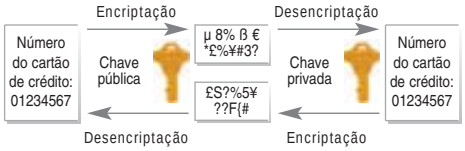
Estas formas de comprometimento de segurança podem não representar uma grande preocupação para um usuário que está simplesmente acessando as páginas de um jornal, revista ou quaisquer outros sites que permitam acesso público irrestrito. Porém, quando informações sigilosas estão em jogo, alguma estratégia para garantir a segurança das comunicações deve ser adotada.

Com esse objetivo, foi desenvolvida uma arquitetura para comunicações sigilosas que deu origem ao protocolo HTTP seguro, ou HTTPS, que é largamente utilizado pelas maiores instituições financeiras, lojas virtuais e todos os tipos de sites que necessitam trocar informações de maneira segura com seus usuários. Este protocolo é capaz de oferecer proteção contra os tipos de comprometimentos de segurança há pouco descritos, através de mecanismos que possibilitam a criptografia, autenticação e verificação de integridade de dados em uma comunicação.

Criptografia

O HTTPS utiliza uma combinação de criptografia simétrica e criptografia de chave pública, ou assimétrica, para garantir a segurança das comunicações. A criptografia simétrica, na qual a chave (segredo) utilizada para encriptar uma mensagem é a mesma usada para desencriptar, tem como vantagem o desempenho, sendo indicada para encriptar grandes volumes de dados.

Na criptografia de chave pública utilizada pelo HTTPS são geradas duas chaves, sendo que cada chave consegue desencriptar o que foi encriptado pela sua chave par. Uma determinada entidade deve gerar seu par de chaves e tornar uma dessas chaves conhecida por todos (chave pública), enquanto a outra chave deve ser mantida sob sigilo (chave privada). Essas características provêm um meio de realizar a autenticação, como veremos a seguir.



Autenticação e Certificados Digitais

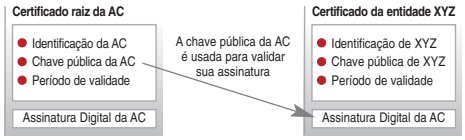
Uma comunicação criptografada garante o sigilo dos dados, mas isto pode não ter o menor valor caso você não tenha meios de garantir a identidade daquele com quem você está trocando informações. Daí, surge a necessidade da autenticação, que é o processo de confirmação de uma identidade.

A autenticação adotada pelo HTTPS utiliza criptografia de chave pública e baseia-se na idéia de que, se uma entidade provar que realmente possui a sua chave privada, sua identidade também estará provada, pois ninguém mais tem acesso a essa chave que, por definição, é sigilosa.

Para realizar essa verificação precisamos da chave pública da entidade a ser autenticada. Mas existe um problema: como podemos garantir que estamos com a chave pública correta dessa entidade?

A solução do HTTPS para essa questão é a utilização de certificados digitais, que funcionam como um documento eletrônico que permite a uma entidade associar sua identificação a uma chave pública.

Os certificados digitais são emitidos por Autoridades Certificadoras (ACs), que devem ser entidades idôneas e confiáveis. Todo certificado deve ser assinado pela AC que o emitiu utilizando a sua chave privada e, a fim de atestar a assinatura contida em um certificado, é necessário o conhecimento da chave pública da AC. Esta chave pública pode ser obtida a partir de certificados especiais, conhecidos como certificados raiz, que normalmente são armazenados no seu computador durante a instalação do browser.



Após o uso dos certificados digitais para realizar a autenticação entre os participantes e garantir que eles estão realmente se comunicando com quem deveriam, é utilizada a criptografia de chave pública para permitir que as partes estabeleçam uma chave simétrica (denominada de chave de sessão), que será utilizada para encriptar os dados transmitidos na comunicação. A partir desse ponto, os dois lados poderão trocar informações em sigilo.

O protocolo HTTPS possui ainda um mecanismo para verificação de integridade de dados, denominado Código de Autenticação de Mensagem (MAC), que é responsável por permitir ao destinatário de uma mensagem verificar se os dados que ele recebeu são idênticos aos que foram enviados pelo remetente.

Pois bem, com a utilização de certificados digitais o HTTPS previne ataques de personificação, através de criptografia usando a chave de sessão evita a escuta e com o uso do MAC permite detectar a adulteração de mensagens.

Verificação de Comunicação Segura

Ao utilizar o seu browser para acessar um serviço na Internet que exija o estabelecimento de uma conexão segura para a transmissão de dados, você deve estar atento aos detalhes que indicam a utilização do protocolo HTTPS. Isto é evidenciado por um endereço Web iniciado com a seqüência "https://".

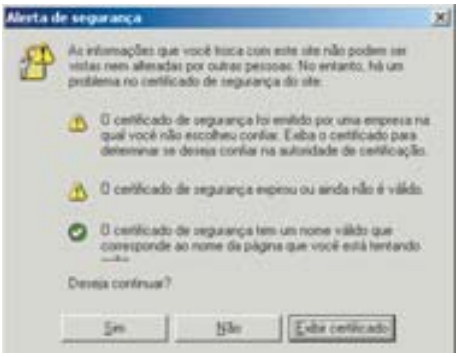
Outra indicação do uso de HTTPS na comunicação é a ilustração de um cadeado, ou de uma chave (isto varia entre navegadores), localizado no canto inferior direito da barra de status do seu browser.

Um cuidado especial também deve ser tomado na verificação dos certificados digitais. Você deve conferir se o endereço do site corresponde realmente ao endereço garantido pelo certificado digital, além de verificar sua data de validade. Para isso, dê um duplo clique na figura do cadeado.

Outros detalhes sobre a conexão segura, como o nível de codificação e os algoritmos criptográficos utilizados, assim como a página que está sendo

acessada, podem ser verificados através da opção "Propriedades" no menu "Arquivos".

Existe ainda outra questão importante sobre certificados que deve ser esclarecida. Caso o seu browser não possua um certificado raiz que valide um certificado de determinada entidade, você será notificado com uma alerta de segurança semelhante ao mostrado na figura abaixo.



Isso não ocorre, por exemplo, com as principais entidades bancárias do país que utilizam certificados emitidos e assinados por ACs conhecidas e confiáveis, naturalmente reconhecidas pelos browsers mais utilizados, que já incluem os certificados raiz dessas ACs desde a instalação.

Ao ser notificado com o alerta acima você deve tomar muito cuidado, pois continuar significa que você estará confiando em um certificado que não é garantido por nenhuma autoridade certificadora reconhecida pelo seu browser. Você também terá a opção, caso exiba o certificado, de instalar o certificado raiz desconhecido na lista de certificados raiz confiáveis e reconhecidos pelo seu browser. Esse é um grande risco, pois, daí em diante, esse certificado raiz recém-instalado poderá validar todos os outros certificados garantidos por ele.

Assim, caso você não tenha total confiança no certificado apresentado, não deve continuar a comunicação, pois há casos de sites clonados que utilizam HTTPS, mas cujos certificados não são garantidos por Autoridades Certificadoras confiáveis.

Nem Tudo Está Seguro

O protocolo HTTPS procura garantir que os dados de uma conexão estarão em segurança por todo o caminho na rede até o seu destino. Mas o risco não existe apenas para os dados em trânsito. A falta de proteção no seu computador pode colocar em risco até mesmo uma conexão aparentemente segura, pois se um hacker estiver infiltrado em seu computador, ele terá acesso às informações confidenciais antes mesmo de elas trafegarem pela rede. Nesse caso, o protocolo HTTPS também se torna vulnerável, pois se um certificado raiz malicioso for instalado, toda a estrutura de verificação de autenticidade de certificados digitais ficará comprometida.

Portanto, você deve tomar diversas precauções que, em conjunto, irão oferecer um maior nível de confiabilidade às suas comunicações que envolvem troca de informações sigilosas via Internet, tendo em mente sempre que a segurança total nunca pode ser atingida. ■

Referências

Dierks, T. e C. Allen. "The TLS Protocol", RFC 2246, Janeiro, 1999.
Melo, L. B. "Funções Unidirecionais e Hash". Revista Perícia Federal, nesta edição.
Rescorla, E. "HTTP Over TLS", RFC 2818, Maio, 2000.
Schneier, B. "Applied Cryptography". 2nd edition, John Wiley & Sons, ISBN 0-471-11709-9, 1996.

Novo portal é sucesso garantido

O site da Associação Nacional dos Peritos Criminais Federais (www.apcf.org.br) passou por uma reformulação geral. No dia 2 de abril deste ano entrou no ar o novo portal da APCF. Com as mudanças efetuadas, os peritos contam agora com uma ferramenta mais ágil de acesso a informações de interesse da categoria. Para saber da satisfação de seu público, a APCF colocou no ar uma enquete. Durante 30 dias, os interessados puderam votar e dizer o que achavam da nova cara do site. O trabalho foi aprovado com louvor. Dos 255 votantes, quase 80% acharam a nova cara do site boa ou muito boa. O trabalho foi executado pelo Designer Waldemar Anton Osmala Júnior, da APCF.

Conferência Internacional

O uso crescente da internet se tornou extremamente propício para o surgimento e crescimento dos chamados crimes cibernéticos. Para discutir assuntos relacionados ao tema acontecerá no início de setembro a I Conferência Internacional de Perícias em Crimes Cibernéticos (ICCyber'2004). O evento, promovido pelo Departamento da Polícia Federal, tem como objetivo fomentar a pesquisa e o desenvolvimento científico da perícia de informática, na busca de se produzirem novas e avançadas técnicas para o combate ao crime. Informações adicionais constam no site do evento www.dpf.gov.br/iccyber2004

Arquivo APCF

Parceria Saúde

A Associação Nacional dos Peritos Criminais Federais - APCF - fechou mais uma parceria para atender melhor seus associados. Pela primeira vez, desde sua criação, a APCF está colocando à disposição dos peritos mais de um plano de saúde. No último dia 22 (abril), os presidentes da Associação, Roosevelt Leadebal Júnior, e da ANSEF (Associação Nacional dos Servidores da Polícia Federal), Carlos Alberto Gatinho, assinaram convênio neste sentido. A parceria vai propiciar aos associados da APCF a oferta de dois planos de saúde: Unimed e Bradesco Saúde.

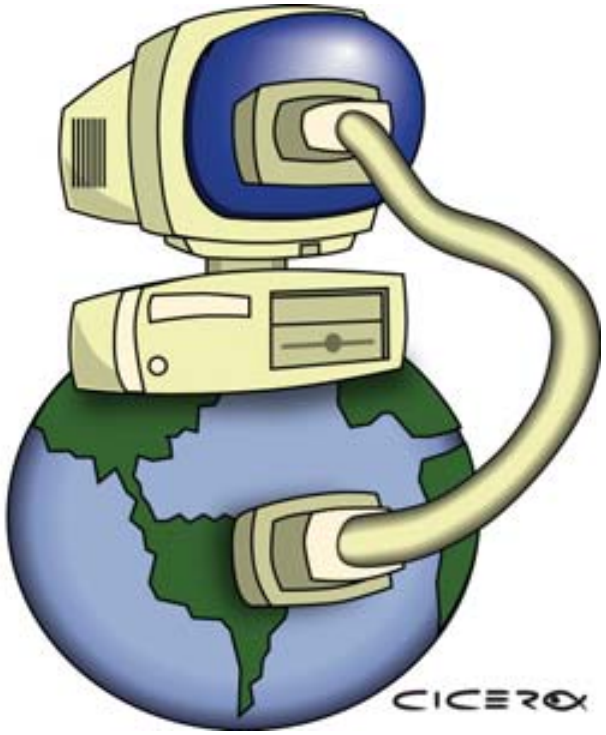
Boa Leitura

O livro do perito Helano Matos chegou para preencher uma lacuna nas referências hoje disponíveis na lingua portuguesa sobre o desenvolvimento orientado a objetos. Combinando a teoria e a prática, o autor discorre sobre o assunto trazendo um vasto material de valor didático. O livro tornou-se indispensável para profissionais e alunos que desejam se especializar em sistemas com ênfase no processo de desenvolvimento de software. A editora é a Edições Livro Ténico.

CAPA: PCF Sérgio Luís Fava (Bacharel em Ciência da Computação)

A Polícia Federal
e o combate aos crimes pela internet

"Criminosos usam várias técnicas para tentar pegar a vítima desprevenida"



No começo de novembro de 2003, a Polícia Federal desencadeou a Operação Cavalo-de-Tróia. Efetuada simultaneamente em diversos estados, resultou na prisão de uma quadrilha especializada em fraudar contas bancárias [1][2]. O método empregado pela quadrilha consistia em enviar falsas mensagens de bancos e pedir informações pessoais, como número de conta e senhas de acesso.

É muito provável que, de um ano para cá, você tenha recebido ao menos uma destas mensagens, supostamente remetida por algum banco, empresa aérea, órgão estatal ou rede de TV. No começo de março, ao escrever este artigo, a Receita Federal era usada como pretexto [3]. Deixaremos para outro artigo o estudo de outras mensagens freqüentemente recebidas por correio eletrônico, a saber:

Vírus: resultado de máquinas infectadas por vírus que ficam enviando mensagens a todos os endereços disponíveis

"Spam": mensagens indesejadas que tentam vender medicamentos, dispositivos para aumentar a potência sexual masculina etc...

"Hoax": são boatos, que disseminam informações inverídicas. Normalmente terminam solicitando o envio de uma cópia para todas as pessoas conhecidas.

Neste artigo, serão examinadas as técnicas empregadas no crime de "phishing", assim chamado pela semelhança com o verbo "fishing", que significa pescar, em inglês. Neste tipo de golpe, tenta-se ludibriar ("pescar") um usuário incauto e convencê-lo a fornecer dados confidenciais.

Estes golpistas são gênios?

É comum pensar que os golpistas tenham profundos conhecimentos de informática e sejam capazes de atacar sistemas bancários diretamente, usando mecanismos de invasão de rede. Neste caso em particular, nenhum banco foi invadido. A técnica empregada foi bem mais simples: remeter, em grandes quantidades, mensagens eletrônicas aos usuários, fingindo ser do próprio banco (figura 1). O texto da mensagem era variável, mas era preparada de tal forma a ser convincente e, ao final, sempre solicitava que o usuário informasse seus dados cadastrais e, principalmente, a senha de acesso.


De: Banco do Brasil
Data: domingo, 4 de janeiro de 2004 16:59
Para: apligral@apligral.com.br
Assunto: Comunicado 2004

Caro cliente BANCO DO BRASIL,

Devido ao grande número de crimes virtuais que vem ocorrendo pela Internet, estamos aqui tentando normalizar nossas atividades. E para isto precisamos conferir os lesados por estes crimes que vem acontecendo. Por favor confira Aqui se sua conta sofreu variações ou transações desconhecidas. Qualquer movimentação deve ser imediatamente comunicada a nossa central de atendimento ao cliente! Ou acesse nosso site! http://www.bb.com.br/

Lembre-se o Banco do Brasil não envia mensagens de correio eletrônico não-autorizadas (spam mail) a seus clientes, nem autoriza qualquer parceiro comercial a fazê-lo em seu nome.

Atenciosamente,
Banco do Brasil

Figura 1
Exemplo de mensagem falsa [4]

Para dar maior aparência de veracidade, algumas técnicas são empregadas para distrair o usuário:

1) Clonagem do site: o golpista cria um site muito parecido com o original, e muda apenas um trecho do endereço (figura 2).
Por exemplo, ao invés de acessar http://www.bb.com.br para acessar o Banco do Brasil, o usuário é levado a acessar um site semelhante mas que, na realidade, está hospedado numa máquina do criminoso, como por exemplo http://www.bb.x.com; o usuário vê a palavra "bb" e pensa que é o site oficial do banco.

2) Redirecionamento de site: o usuário vê a janela real do banco, mas acima dela aparece outra janela pedindo as informações para acesso; os dados, ao invés de irem para o banco, vão para o site do golpista.

3) Exploração de falhas dos navegadores da Internet [5]:
no final de 2003, foi descoberta uma falha no Internet Explorer que poderia acarretar a visualização de um endereço na barra de endereços ao mesmo tempo em que o site mostrado era outro! Quer saber se o seu browser sofre deste problema?
Verifique a referência [6].

4) Obscuração de endereço: se você digitar o seguinte endereço no browser, qual site será acessado http://www.bb.com.br@www.bandido.com? As regras de formação de endereço fazem com o que vem antes do sinal "@" seja desconsiderado; o site real é http://www.bandido.com.
Outras combinações também são possíveis, sendo muitas vezes difícil interpretar de maneira simples o significado do endereço.

5) Como mostra a Figura 3, é possível criar uma mensagem que mostre um link insuspeito, mas cujo endereço verdadeiro é um site criado pelo criminoso. Trata-se de um truque muito simples, pois muitos usuários não têm o hábito de olhar o endereço real que aparece na parte de baixo da janela.

Como então se proteger?

Nas referências [7], [8] e [9], você pode encontrar algumas dicas de segurança em geral.

Figura 2
Falso site do banco [10]

Figura 3
Um link apontando para site diferente

No caso destas mensagens falsas, esteja sempre desconfiado.

Não responda nenhum e-mail, sem antes acessar o site de seu banco e conferir as informações. Se preferir, procure o gerente ou a central de atendimento aos clientes.

Rastreamento de uma denúncia leva à Itália

Onde ficam os sites piratas?

Normalmente em máquinas desprotegidas de outros países, como a perícia em informática do Instituto Nacional de Criminalística pôde constatar. Em setembro/2003 um dos peritos recebeu uma mensagem falsa de banco. Imediatamente, efetuamos o rastreamento, e verificamos que os dados a serem digitados iriam para um site na Itália. Entramos em contato com o administrador do site, que, após demonstrar surpresa, bloqueou o acesso indevido. Foi possível descobrir, ainda, para onde os dados eram redirecionados. Isto, infelizmente, é uma característica da internet: um criminoso tem, a seu dispor, grande número de máquinas no mundo inteiro que não estão devidamente protegidas; e as usa para instalar sites e dificultar bastante o rastreamento das informações [11].

Como descobriram seu e-mail?

Ao receber mensagens de origem desconhecida, muitos usuários se perguntam: como conseguiram meu endereço? Será que alguém anda me vigiando, e através de espionagem obteve estas informações?

Nada tão dramático

Você foi apenas vítima de alguma das técnicas de obtenção em massa de endereços:

1) Garimpagem:
Trata-se de percorrer páginas e e-mails, procurando a letra "@", selecionando a palavra antes e depois desta letra origina, muito provavelmente, um endereço válido.

2) Força bruta:
Onde são tentadas várias combinações em seqüência. As mensagens são enviadas para todos os endereços da forma a@mail.com, b@mail.com, c@mail.com, ..., aa@mail.com, ab@mail.com, ac@mail.com e assim por diante.

3) Método do dicionário:
Consiste em selecionar nomes e palavras mais comuns a partir de uma lista pré-definida, tais como joao@mail.com, gerente@mail.com, imprensa@mail.com e assim por diante.

4) A maneira mais fácil, contudo, é comprar listas de e-mail diretamente. Com poucas centenas de reais, é possível adquirir, na Internet, CDs com milhões de endereços.

Mas será que vale a pena tanto trabalho?

Se fosse feito de forma manual, com certeza seria impraticável. Porém, constata-se aqui uma das marcas registradas dos crimes praticados com o uso da Internet: a automação dos ataques, ou seja, a capacidade de executar tarefas de grande escala sem quase nenhuma intervenção humana; todo o trabalho pesado é feito através de programas de computador, que podem ficar horas a fio coletando informações e enviando mensagens.

Da mesma forma, este tipo de crime permite que o criminoso nem se importe se a maioria das mensagens não tiver destinatário válido. Neste tipo de "negócio" é muito barato enviar mensagens. O importante é que algumas pessoas respondam, o que já garante retorno financeiro.

Aliás, a perícia federal detectou outro fato preocupante: além dos e-mails, os golpistas também vendiam um "kit" com todos os programas e listas de sites desprotegidos. Desta forma, outras pessoas tiveram acesso à "tecnologia" e passaram a aplicar estes golpes também.

Há alguma coisa de pessoal contra você?

Ao receber uma mensagem destas, muitos se perguntam: seria um crime tramado especialmente contra mim? Diferentemente de um assalto à mão armada, por exemplo, em que você é "escolhido" entre outros, a filosofia por trás destes golpes via internet é impessoal: mensagens tentando ludibriar dezenas de milhares de pessoas são enviadas por alguém que não tem o menor conhecimento de suas vítimas.

De quem é a culpa?

Não faltam pessoas para dizer que os responsáveis por esta situação são os fabricantes de software (que criam programas inseguros), os bancos (que não estariam protegendo os correntistas adequadamente) e até os usuários, que saem clicando em tudo que vêem pela frente.

Os bancos não deveriam estar fazendo algo para proteger seus correntistas? Sem entrar no mérito da segurança bancária, este é um tipo de golpe difícil de ser evitado. Pense numa situação da vida real: é possível impedir que alguém envie uma carta e coloque o nome de outra pessoa como remetente? Não, é impossível, da mesma forma que no mundo das redes informatizadas uma empresa pública ou privada não tem como prevenir este golpe.

Nós, da Perícia Federal, não temos a menor dúvida: a culpa é dos criminosos que exploram a boa-fé e a falta de conhecimento dos usuários, os quais, na maioria das vezes não estão treinados para distinguir um endereço verdadeiro de um falso.

Se você foi vítima de um golpe destes, faça o devido registro policial, comunique o banco e exija providências. Não caia no jogo daqueles que querem culpar a vítima e esquecem da vilanice dos autores, verdadeiros estelionatários do mundo virtual.

Conclusão

É sempre difícil antecipar o que está por ocorrer, mas tudo indica que, num futuro próximo, este tipo de golpe ainda vai ser muito explorado. Novos truques ainda surgirão, exigindo cada vez mais empenho e o desenvolvimento de novas técnicas de investigação. ■

Referências

[1] PF prende acusados de integrar quadrilha que hackers no Piauí - http://www1.folha.uol.com.br/folha/cotidiano/ult95u86250.shtml
[2] PF prende crackers que desviaram R$ 100 milhões - http://info.abril.com.br/aberto/infonews/112003/06112003-3.shl
[3] Golpe usa nome da Receita Federal para enganar internautas - http://www1.folha.uol.com.br/folha/informatica/ult124u15398.shtml
[4] Cópia da mensagem falsa - http://www.infoguerra.com.br/infonews/fotos/golpes/bb_bug_msg.gif
[5] Golpe por e-mail tenta explorar novo bug do IE - http://www.infoguerra.com.br/infonews/viewnews.cgi?newsid1073443984,69626,/
[6] Internet Explorer URL Spoofing Vulnerability (estes sites podem ser bloqueados por seu programa antivírus, que impedirá a realização do teste). Ambos estão em inglês.
http://www.secunia.com/internet_explorer_address_bar_spoofing_test/ e http://www.zapthedingbat.com/security/ex01/vun1.htm
[7] Cartilha de Segurança para Internet - NIC BR Security Office - http://www.nbso.nic.br/docs/cartilha/
[8] O que você precisa saber sobre sites mal-intencionados - http://www.microsoft.com/brasil/security/sitesfalsos.asp
[9] Segurança no uso da Internet - Febraban (Federação Brasileira dos Bancos) - http://www.febraban.org.br/Arquivo/Servicos/Dicasclientes/dicas7.asp
[10] Cópia de uma página falsa - http://www.infoguerra.com.br/infonews/fotos/golpes/bb_th.gif
[11] Your computer could be a 'spam zombie': http://www.cnn.com/2004/TECH/ptech/02/17/spam.zombies.ap/index.html

Peritos:
o fortalecimento da categoria

O primeiro encontro de grande porte realizado pela APCF teve participação de 85 peritos

O I Encontro Nacional dos Peritos Criminais Federais, que aconteceu em Porto Seguro, entre os dias 27 e 30 de abril, reuniu representantes de vários estados.

Profissionais mais e menos experientes aproveitaram o evento para trocar idéias e fortalecer o espírito da categoria. Aliás, o fortalecimento da união dos peritos foi considerado o principal resultado do evento, na opinião do presidente da Associação Nacional dos Peritos Criminais Federais, Roosevelt Júnior. "O início de um discurso único será sentido não só pelo Departamento de Polícia Federal, como também pela sociedade", afirmou ele.

A categoria de peritos conta hoje com 444 profissionais distribuídos em diversas áreas. Este número deve praticamente dobrar com o novo concurso anunciado pelo governo federal para a contratação de pelo menos mais 506 profissionais.

Ernesto Reich

Peritos debateram vários assuntos durante o primeiro encontro da categoria em Porto Seguro

Grupos de Trabalho

Foram quatro dias de reuniões onde os temas escolhidos foram debatidos exaustivamente. Os peritos se dividiram em três grupos de trabalho: Projeto de Perícia, Lei Orgânica e Trabalho dos Aposentados. Os resultados destas discussões foram votados pela Assembléia Geral Extraordinária.

Dentre os pontos discutidos pelos aposentados está a manutenção do compromisso da equiparação salarial entre peritos na ativa e aposentados.

Leia ao lado as principais propostas definidas pelo grupo:

Aposentados

Participação dos Peritos aposentados em cursos realizados pela Academia Nacional de Polícia (ANP). Principalmente nos cursos de formação de peritos criminais federais.

Ter como objetivo e compromisso a manutenção da equiparação salarial entre ativos e aposentados.

A APCF deve fazer um histórico do Instituto Nacional de Criminalística (INC) ouvindo os peritos desde sua fundação até o momento.

Lei Orgânica

O grupo de trabalho que desenvolveu o tema sobre lei orgânica teve como base as três propostas de lei orgânica que já são conhecidas. Os temas discutidos foram: propostas de Cargo Único para o Departamento de Polícia Federal (DPF); modos de ingresso no cargo de Perito Criminal Federal (PCF); prerrogativas e atribuições do Perito Criminal Federal; composição do conselho de ética e disciplina; ocupação de cargos de administração policial por Peritos Criminais Federais; figura do "Policial Natural"; e choque de atribuições dentro e fora do DPF.

Quanto ao projeto de perícia ficaram definidas propostas como a criação de unidades de perícia nas delegacias e o fortalecimento da categoria

Projeto da perícia

1. Constitucionalização da perícia em cooperação com a ABC e outras entidades de classe;

2. Extinção do perito ad hoc;

3. Trazer a identificação papiloscópica para a criminalística;

4. Integrar as atividades do NID dentro dos Setec's;

5. Busca de soluções para racionalizar os Laudos Merceológicos, de transcrição fonográfica e os pareceres técnicos para exames em moeda;

6. Aumentar o número de peritos para no mínimo, o correspondente a 10% do efetivo do DPF;

7. Criação de unidades de perícia nas delegacias;

8. Dotação de um mínimo necessário de recursos materiais para cada unidade da perícia;

9. Dotação de um número mínimo necessário de peritos em cada unidade da perícia;

10. A definição de um contingente da carreira de apoio administrativo destinado à criminalística para auxiliar nos examese nas atividades de administração das unidades da perícia;

Resultados

O primeiro encontro nacional dos peritos criminais federais reuniu 85 profissionais. A expectativa do presidente da APCF é de que no ano que vem o número de participantes passe dos 100. Se depender do entusiasmo demonstrado pelos peritos que estavam neste primeiro encontro, o próximo, com certeza, vai ser um sucesso. A segunda reunião, já tem data e local definidos. Os peritos resolveram que Bonito (no Mato Grosso do Sul) será o local para o novo encontro, que acontecerá em abril de 2005. ■

CARTA DE PORTO SEGURO

Vivemos um momento de extrema gravidade na área de segurança pública. A impunidade somada à problemática social são os grandes responsáveis pelo elevado índice de criminalidade em nosso país.

O exemplo das nações que tradicionalmente investem na polícia científica evidência os resultados positivos na redução da criminalidade, nos indicando o caminho a ser seguido.

À conjuntura nacional são acrescidos o problema do pleito por melhores condições de trabalho e reconhecimento profissional de toda categoria Policial Federal, expressos por meio das recentes reivindicações junto ao poder público. Embora munidos de formação técnico-científica de excelência e do entusiasmo pelo trabalho de materialização das provas de crimes, os Peritos Criminais Federais carecem de aparelhamento tecnológico e infra-estrutura para realizar, com eficácia, as perícias nas áreas do crime financeiro, engenharia, análises químicas, audiovisuais, biológicas, ambientais, de informática, documentoscópica e inúmeras outras.

A despeito de tal conjuntura, os atuais 444 peritos do Departamento de Polícia Federal DPF foram responsáveis pela elaboração, em 2003, de 29.582 laudos, com perícias em diversas áreas da criminalística, bem como pela produção científica de novos métodos e alternativas para o combate ao crime, contribuindo decisivamente para o desenrolar de inquéritos policiais e processos judiciais, a exemplo dos casos Banestado, TRT de São Paulo, SUDAM/SUDENE e Operação Anaconda. Mesmo com todo o trabalho realizado pelos profissionais ainda restam no Brasil 8.202 pendências de análises periciais reforçando com isso a necessidade de um significativo incremento no quadro de Peritos Criminais Federais, associado aos investimentos em equipamentos que possam fazer frente à sofisticação das organizações criminosas.

Diante desse contexto e no intuito de apresentar sugestões à solução do problema, a Associação Nacional dos Peritos Criminais Federais - APCF promoveu o I Encontro Nacional dos Peritos Criminais Federais, no período de 27 a 30 de abril de 2004, em Porto Seguro/BA, onde foram deliberadas as seguintes propostas a serem encaminhadas em caráter de urgência:

· Aprovação da Lei Orgânica da Polícia Federal, onde se conciliem os pleitos dos integrantes da carreira Policial Federal;

· Reorganização administrativa do DPF, de forma que os setores voltados à atividade pericial tenham o mesmo tratamento hierárquico dispensado aos demais setores de atuação da Polícia Judiciária da União; e

· Reaparelhamento da Polícia Federal, em especial da perícia, com a implantação dos Projetos PROMOTEC e PROAMAZÔNIA, nos moldes inicialmente previstos.

Esperamos com isso dar um passo decisivo para transformar a Polícia Federal no órgão de excelência que a sociedade deseja, capaz de cumprir suas funções constitucionais de forma eficiente e eficaz.

Os peritos criminais federais sempre acreditaram e acreditam em uma ÚNICA Polícia Federal.

PERITOS CRIMINAIS FEDERAIS

Funções Unidirecionais e Hash

"Da integridade de documentos às assinaturas digitais, elas estão por trás de boa parte dos conceitos envolvidos na segurança de dados"

Ao fazer uma aposta na loteria recebemos um bilhete com os números escolhidos e sabemos que, se eles forem sorteados, o prêmio só será pago se este mesmo bilhete for apresentado aos responsáveis. Da mesma forma, um extrato bancário de uma conta qualquer pode ser apresentado como comprovante de saldo no caso de "desaparecimento" de qualquer quantia. Mas como as instituições lotéricas e bancárias fazem para descobrir se aquele bilhete premiado ou aquele extrato com um saldo milionário não foram forjados?

Por outro lado, imagine uma transmissão de dados que envolva valores importantes. Por exemplo, a comunicação entre um terminal de saques e o computador central do banco. O que aconteceria se alguém conseguisse interceptar essa comunicação e alterasse o valor dos saques efetuados? Não seria nenhuma surpresa se saques de R$ 1.000,00 passassem a ser registrados como de apenas R$ 1,00...

Em todos os casos citados, as chamadas Funções Unidirecionais podem ser ferramentas de extrema utilidade para solucionar problemas, sejam eles a garantia de autenticidade de documentos ou a busca de integridade nas comunicações.

O que são Funções Unidirecionais?

O conceito é bastante amplo. De forma geral, podemos definí-las como aquelas funções fáceis de calcular, porém difíceis de serem revertidas. Um quebra-cabeça de 1 milhão de peças, por exemplo, pode ser considerado como uma função unidirecional: é muito fácil desmanchar, porém pouco encorajador montar novamente.

Matematicamente falando, são funções para as quais o cálculo da imagem de um determinado elemento do domínio, em termos práticos, tem baixo custo computacional, mas a determinação deste elemento a partir da imagem é inviável. Ou seja: se aplicarmos uma função unidirecional sobre um número qualquer, obteremos o resultado após alguns cálculos relativamente simples. Porém, se conhecermos apenas o resultado e tentarmos descobrir o número que o gerou, poderiam ser necessários milhares de supercomputadores trabalhando por milhões de anos. A partir desta idéia aparentemente simples, foi possível construir muitos dos mais complexos conceitos criptográficos atuais.

Para que servem?

A despeito das várias utilidades já comentadas, as funções unidirecionais, por si só, não oferecem muitas vantagens para a aplicação mais conhecida da criptografia, que é a de cifrar e decifrar documentos. Podemos até cifrar um documento com uma função unidirecional, porém o resultado será de uma inutilidade completa. Afinal, seremos incapazes de decifrá-lo posteriormente devido à propriedade de não-reversibilidade já explicada. Para este caso, entretanto, existe um tipo especial de Função Unidirecional chamado Trapdoor. Uma função deste tipo possui um segredo que torna fácil àquele que o conhece realizar a operação inversa da mesma, possibilitando a criação de esquemas robustos de criptografia como o da assinatura digital. Este assunto, no entanto, tem tanto a ser explorado que será tema de artigos futuros.

Aqui, trataremos de um outro tipo especial de funções unidirecionais, as chamadas Funções de Hash (mistura, em inglês). Centrais na criptografia moderna, as funções unidirecionais de hash têm aplicação nas mais variadas situações, inclusive aquelas citadas nos parágrafos iniciais deste artigo. Vamos conhecer melhor o funcionamento destas funções antes de comentar algumas de suas aplicações específicas.

As chamadas Funções Unidirecionais podem ser ferramentas de extrema utilidade para solucionar problemas, sejam eles a garantia de autenticidade de documentos ou a busca de integridade nas comunicações

Funções Unidirecionais de Hash

Uma Função de Hash tem a propriedade de transformar um conjunto de dados de entrada de qualquer tamanho em um outro conjunto de dados de tamanho fixo, normalmente menor que a entrada. Um determinado conjunto de dados sempre produzirá o mesmo valor de Hash, e qualquer alteração no mesmo, por menor que seja, deverá produzir um valor diferente. Se esta função tiver ainda uma propriedade que garanta a inviabilidade de se realizar o processo inverso, ou seja, determinar o conjunto de dados original a partir do valor de Hash, ela será então uma Função Unidirecional de Hash.

Na prática, as Funções Unidirecionais de Hash são chamadas simplesmente de hash, bem como o valor que é calculado por elas.

Grosso modo, podemos dizer que uma Função de Hash é capaz de calcular resumos de conjuntos de dados. Elas podem ser comparadas a uma máquina em que, de um lado, entram os dados (que podem ser um documento de texto, uma música, uma imagem ou qualquer outro arquivo) e, do outro lado, sai um número que o representa (o valor de hash). Embora este número possa ser obtido a partir de mais de um conjunto de dados (colisão), é essencial a uma Função de Hash que seja inviável a escolha de dois conjuntos de dados que produzam o mesmo hash ou de um conjunto de dados que resulte em um valor de hash específico.

Atualmente, estes requisitos são perfeitamente atendidos pelos algoritmos de implementação de Hash mais utilizados, como o MD5 e o SHA. O MD5, por exemplo, pode produzir 2^{128} valores de hash diferentes. Para se ter uma idéia deste número, ele é 100 trilhões de vezes maior que a quantidade de grãos de areia do Deserto do Saara.

Como não há nenhum método conhecido para se obter valores de hash específicos, uma pessoa que quisesse encontrar um conjunto de dados capaz de gerar um valor particular de hash teria que fazer tentativas aleatórias. Se esta pessoa estivesse disposta a gastar 1 milhão de dólares comprando equipamentos de última geração, seriam necessários, em média, 10^{16} anos para atingir seu objetivo - detalhe: este tempo é 1 milhão de vezes maior que a idade estimada do universo. Existe, é claro uma chance de se acertar na primeira tentativa, mas ela é tão pequena que seria mais fácil ser atingido 3 vezes por um raio e ainda acertar na Mega Sena - isso tudo num mesmo dia.

Um aspecto interessante do uso das Funções de Hash mais utilizadas é que não há segredos no seu mecanismo. Os cálculos efetuados para se determinar um valor de hash são de conhecimento público, e foram submetidos a toda sorte de análises para a verificação de sua robustez. Mesmo sem senhas ou segredos de qualquer tipo, não há como realizar o processo inverso. A segurança está na sua propriedade de não-reversibilidade.

Garantindo a integridade de dados

A grande utilidade do uso das Funções de Hash é a possibilidade de se garantir a integridade de dados, seja durante o seu armazenamento ou a sua transmissão. Uma vez que um valor de hash representa o conjunto de dados a partir do qual ele foi calculado, podemos, a qualquer momento, calcular novamente o hash deste mesmo conjunto de dados e comparar com o valor obtido originalmente. Em termos práticos, uma coincidência de valores garante que o conjunto de dados não sofreu alterações, enquanto a divergência dos mesmos revela que houve alguma alteração, por menor que ela seja. As Funções de Hash são tão sensíveis a alterações que a mudança de um único bit na mensagem de entrada faz com que pelo menos a metade dos bits do hash sejam alterados. Como exemplo, temos na Tabela 1 os valores de hash calculados para dois textos que se diferenciam apenas pela letra inicial maiúscula e minúscula: podemos observar que seus respectivos valores de hash são completamente distintos.

Texto	Hash
Teste de hash - texto para comparação de valores de hash	`b81400c2323a29a1e055c53a9833b658`
teste de hash - texto para comparação de valores de hash	`e403e461007861fa17cd185360efbf62`

Tabela 1 - Exemplo de aplicação do algoritmo MD5

Garantindo a autenticidade de dados

Como já foi dito, os cálculos envolvidos nas Funções de Hash mais utilizadas são de conhecimento geral. Qualquer um pode calcular o hash de qualquer coisa. Entretanto, é possível restringir tanto a capacidade de geração quanto de verificação dos hashes àqueles que detenham a posse de um segredo. Isto é feito concatenando-se uma senha ao final do conjunto de dados antes de se calcular o seu hash, de forma que somente aqueles que souberem o que deve ser concatenado conseguirão calcular os valores esperados.

Desta forma, é possível construir mecanismos de autenticação que sejam particularmente úteis em casos como aqueles citados no início do artigo. Um bilhete de loteria, por exemplo, pode conter um valor de hash calculado a partir dos números marcados pelo apostador concatenados com uma senha secreta, armazenada na máquina impressora. Se algum trapaceiro tentar forjar um bilhete ganhador, ele não saberá como gerar o valor correto de hash, pois precisaria concatenar a senha secreta aos números sorteados. Logicamente, a casa lotérica poderá perceber a fraude facilmente.

O mesmo mecanismo também pode ser utilizado nos extratos bancários e nas transmissões seguras de dados: se alguém tentar adulterar as informações, não conseguirá gerar os códigos de autenticação corretos para os dados falsos.

Decidindo se uma senha digitada é correta sem conhecê-la previamente

Sistemas operacionais como o Windows e o Linux têm um arquivo que é consultado sempre que algum usuário tenta acessar o sistema (fazer o login), ocasião em que é verificado se aquele usuário é válido e se ele digitou corretamente a senha. À primeira vista, é de se supor que este arquivo contenha uma lista com os nomes de todos os usuários e suas respectivas senhas, o que permitiria ao sistema compará-la com o que foi digitado pelo usuário. Contudo, este modelo teria uma grave vulnerabilidade: se um invasor conseguisse acesso a este arquivo, ele saberia a senha de todos os usuários e, conseqüentemente, teria acesso total ao sistema.

O uso das funções de hash, entretanto, possibilita a construção de uma segunda opção para o processo de autenticação dos usuários, que inclusive é a adotada pelos sistemas citados. Ao invés de guardar as senhas dos usuários, o arquivo em questão contém apenas os valores de hash dessas senhas. Desta forma, quando um usuário faz o login, o sistema calcula o hash da senha digitada e compara com o valor guardado no arquivo.

A grande vantagem desta segunda opção é possibilitar que as senhas dos usuários não precisem ser armazenadas pelo sistema. Mesmo que alguém tenha acesso ao referido arquivo, não conseguirá descobrir as senhas do usuário a partir de seus valores de hash (afinal, eles são o resultado de funções unidirecionais). Em algumas versões anteriores dos sistemas Linux, inclusive, este arquivo era público, de acesso irrestrito.

O Hash e a Assinatura Digital

A assinatura digital em documentos eletrônicos, tão em voga atualmente, tem o objetivo de se aproximar da assinatura de próprio punho utilizada em documentos escritos ou impressos. Sua utilização tem sido cada vez mais difundida, mas sua praticidade estaria comprometida sem o uso dos hashes. De maneira simplificada, assinar digitalmente um arquivo consiste em cifrá-lo com a chave privada do assinante. A verificação da assinatura, por sua vez, consiste em decifrar este arquivo através da chave pública correspondente. A amarração entre pessoa e documento é viabilizada através do par de chaves utilizado para cifrar e decifrar o arquivo e se baseia nos sistemas de criptografia de chave pública comutativos, onde uma das chaves inverte o papel da outra.

Assinar documentos eletrônicos desta forma, no entanto, apresenta duas grandes desvantagens:

- O documento assinado fica ilegível, pois está cifrado; se alguém quiser lê-lo, terá que conhecer a chave pública do assinante e usá-la para a decifragem;
- O processo de assinatura digital de um arquivo requer uma apreciável quantidade de cálculos complexos, necessitando de uma parcela considerável de tempo para ser executado.

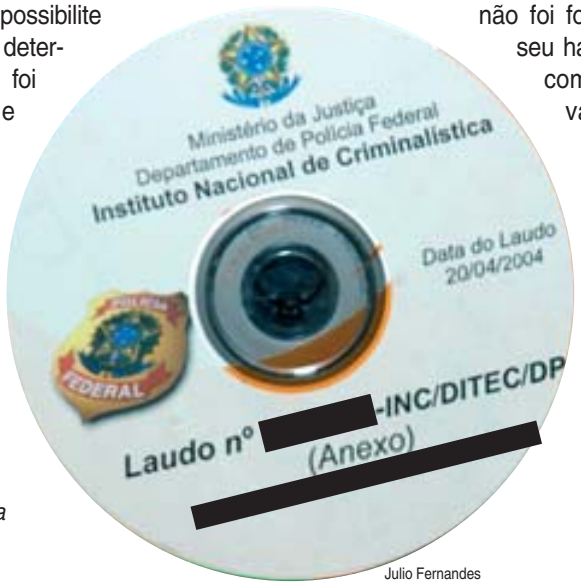
O uso das Funções de Hash na Perícia Federal

Muitos dos laudos periciais emitidos pela Polícia Federal são acompanhados de um anexo em CD-ROM. Este é o caso dos laudos de informática, que comumente precisam ser acompanhados de planilhas eletrônicas, imagens digitalizadas e bancos de dados, dentre vários outros tipos de arquivos cuja visualização depende da utilização do computador. Com essa forma de apresentação, recursos como a facilidade de manipulação de grandes volumes de informações, rápida navegação pelos documentos, buscas por palavras-chave e simulações, ordenação e cálculos com valores, entre outros, tornam a análise dos resultados da perícia uma tarefa menos penosa.

Surge, todavia, um problema de segurança: ao contrário do que ocorre nos documentos em papel, adulterações em arquivos de computador não deixam sinais aparentes. Podemos verificar com certa facilidade se um texto foi rasurado ou apagado, mas não temos como verificar, simplesmente analisando um arquivo, se algum de seus bits foi trocado. Ainda que os discos utilizados pela perícia não permitam a regravação dos dados, faz-se necessário um mecanismo que possibilite garantir que um determinado CD não foi simplesmente substituído por outro contendo dados forjados.

Uma saída seria utilizar as cópias que são arquivadas no Instituto Nacional de Criminalística para comparar com os arquivos dos CDs sob suspeita. Embora tal procedimento possa efetivamente ser utilizado, ele não é nem um pouco prático. Imagine os custos e o tempo gasto para se enviar à perícia os CDs de laudo sempre que se desejar verificar se são íntegros.

Neste caso, o uso das Funções de Hash resolve de forma prática e satisfatória o problema da integridade dos dados. Ao gravar um CD, o perito criminal gera um arquivo de verificação contendo uma lista de nomes de todos os outros arquivos e seus respectivos valores de hash calculados. Este arquivo é incluído no CD e também tem o valor de hash calculado, que é impresso no laudo em papel. Desta forma, qualquer pessoa é capaz de verificar a integridade de um CD de laudo, pois basta a ela calcular os hashes dos arquivos contidos no CD e comparar com os valores armazenados no arquivo de verificação. Se houver qualquer discrepância, está comprovado que algum arquivo foi alterado, mas, se todos os valores coincidirem, é preciso ainda verificar se o próprio arquivo de verificação não foi forjado. Para isso, seu hash é calculado e comparado com o valor que consta no corpo do laudo impresso, que por sua vez é assinado pelos peritos criminais. ■



Exemplo de um CD-ROM de laudo pericial emitido pela Polícia Federal

Julio Fernandes

Referências

Applied Cryptography, 2nd edition, Bruce Schneier, John Wiley & Sons, 1996

Criptografia e Segurança na Informática, Pedro A. D. Rezende, Ciência da Computação - Universidade de Brasília

Autentificação, Computer Emergency Response Team - RS, http://www.cert-rs.tche.br/docs_html/autentic.html e http://www.bgsu.edu/departments/chem/faculty/jtodd/chem100/sp2003/supp/sahara.pdf

Vídeo dá aula
sobre trabalho dos peritos

O trabalho dos peritos criminais federais envolve diversas áreas do conhecimento

Para que serve o trabalho da perícia? Qual sua importância para a segurança dos cidadãos e na busca de soluções eficientes e eficazes no combate à criminalidade? No intuito de responder essas perguntas, a Associação Nacional dos Peritos Criminais Federais (APCF) produziu um vídeo institucional que conta a importância do trabalho da perícia e suas áreas de abrangência.

Com o vídeo fica claro qual é a função da perícia, que é a de processar vestígios e indícios, interpretando-os e elaborando o laudo pericial. Este laudo vai dar suporte ao processo de investigação criminal e a posterior denúncia do Ministério Público.

Para entender a importância do trabalho realizado pelos peritos é bom ressaltar que o processo criminal é baseado em provas e a prova pericial é reconhecida como a "rainha" das provas.

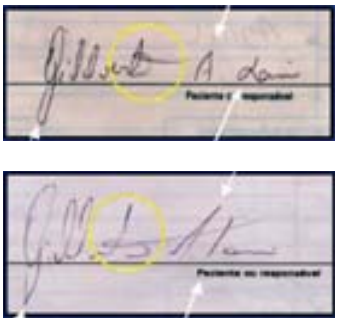
Muitas pessoas não conhecem o trabalho dos peritos e nem imaginam de que forma é feita a apuração de informações que, posteriormente, serão colocadas no laudo pericial. Os profissionais que trabalham na elaboração destes dados são das mais diversas áreas. Você poderá encontrar peritos formados em química, física, engenharia civil, elétrica, eletrônica, mecânica e florestal, agronômica e de minas, ciências contábeis, econômica e biológica, geologia, farmácia, medicina, humana e veterinária, bioquímica e computação cientifica.

Arquivo APCF

Bombas e explosivos fazem parte do trabalho dos peritos. Profissionais periciam carro com bomba.

Descobrir a falsificação de papel moeda faz parte do trabalho dos peritos. Na foto acima, as diferenças entre nota verdadeira e falsa de cinco reais

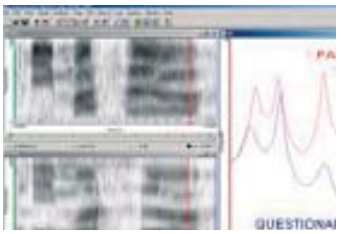
Documentoscopia



A área de documentoscopia, entre outros trabalhos, analisa a falsificação de assinaturas, como na imagem acima

Fotos: Arquivo APCF

A Balística Forense analisa armas usadas em crimes. Informações como munições e defeitos de disparos podem ser descobertas durante a perícia



Equipamentos sofisticados fazem a chamada verificação de locutor para confirmar vozes captadas em escutas telefônicas ou gravações.

Áreas da perícia

O vídeo mostra de forma detalhada as diversas áreas de atuação dos peritos.

No serviço de crimes financeiros, os profissionais são especializados em combater a corrupção, lavagem de dinheiro, crimes contra ordem tributária, sistema financeiro nacional e administração pública. A perícia financeira examina movimentações bancárias, declarações de impostos de renda e balanços patrimoniais.

Alguns dos casos que passaram pelo crivo dos peritos e que tiveram grande repercussão nacional são os do Banco Nacional, TRT de São Paulo e Banestado.

Outra área de atuação dos peritos é de audiovisual e eletrônicos. Os profissionais desenvolvem um minucioso trabalho de análise de gravações de áudio e vídeo – para verificar edições e montagens –, exames em centrais telefônicas clandestinas e grampos telefônicos.

Os crimes ambientais também são alvo de investigação por parte dos peritos. Por ser de natureza complexa e multidisciplinar, a investigação deste tipo de crime exige a atuação conjunta de profissionais de diversas áreas.

Podemos relacionar entre os crimes ambientais o desmatamento, incêndios florestais, poluição, extração mineral irregular, tráfico de animais silvestres e crimes contra o patrimônio histórico e artístico. Um bom exemplo do trabalho realizado pelos peritos e que ficou conhecido em todo o país foi a solução do caso do rompimento da barragem de resíduos industriais da indústria Cataguazes de papel, de Minas Gerais.

Mas a perícia ainda tem atuação em muitas outras áreas importantes. O superfaturamento de obras, processos licitatórios fraudulentos e grilagem de terra são crimes investigados pelo serviço de engenharia legal. O caso de irregularidade em financiamentos da Sudam e Sudene é um exemplo de investigação realizada pelos peritos desta área.

Exames de DNA, hoje, estão na moda. Este exame se tornou uma das mais modernas e eficientes ferramentas à disposição da perícia para elucidar crimes. Podem ser examinados nesta vertente desde fios de cabelo, guimba de cigarro até manchas de sangue e sêmen. Quem não se lembra do caso de paternidade do filho da cantora mexicana Glória Trevi? Foi por meio de um exame de DNA que este caso foi solucionado.

A documentoscopia, outra área de atuação dos peritos federais, identifica processos e métodos utilizados na falsificação de assinaturas, passaportes, títulos da divida pública e papel moeda.

Como identificar a rota utilizada pelo tráfico de armas? Os responsáveis por este trabalho são os peritos da balística forense. Os policiais verificam, por meio de análise de armas de fogo, elementos que compõe munições e defeitos de disparos. Exames minuciosos podem detectar a trajetória e a distância do disparo.

O combate às drogas e o controle de produtos químicos também estão incorporados ao trabalho dos peritos da Polícia Federal. No laboratório de química forense é possível, por meio de exames, identificar as várias formas de apresentação de diferentes drogas existentes no mercado e seus teores. É possível ainda determinar princípios ativos de medicamentos.

Mas o trabalho da perícia não pára por aí. Os peritos se dedicam ainda a solução de crimes cibernéticos, examinando equipamentos de informática para solucionar casos que envolvem investigações no espaço virtual. Cabe aos profissionais realizar auditorias em sistemas bancários, rastrear hackers e sites ilegais, como por exemplo sites de pedofilia.

E por último, existe ainda o trabalho com bombas e explosivos. Os peritos executam atividades de vistoria na busca de material suspeito, transporte e desativação, destruição de objeto suspeito e ainda coleta de vestígios em local de explosão.

Difundindo a atuação dos peritos

Assistindo ao vídeo é possível acompanhar a gama de trabalho dos peritos criminais federais e suas diversas áreas de atuação no combate a crimes de toda a ordem. A diretoria da APCF pretende difundir este vídeo em diversos setores da sociedade para mostrar a importância do trabalho dos peritos e seu papel crucial na defesa da segurança pública do país. ■

Crimes cibernéticos e seus efeitos multinacionais

"A característica dos crimes cibernéticos que mais dificulta o seu combate é o fato de não existirem fronteiras para sua consecução"

"Para que o combate a esses crimes possa ser eficaz e também eficiente, principalmente quando são praticados ou têm efeito em vários países, mister se faz a cooperação internacional por meio de entidades organizadas e estruturadas para esse fim"

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

Nesse diapasão, para que o combate a esses crimes possa ser eficaz e também eficiente, principalmente quando são praticados ou têm efeitos em vários países, mister se faz a cooperação internacional por meio de entidades organizadas e estruturadas para esse fim. Além disso, é importante fomentar a pesquisa e o desenvolvimento no âmbito da perícia de informática.

Visão geral dos crimes cibernéticos

Os crimes por computador são gênero do qual os crimes cibernéticos são espécie, i.e., os crimes cibernéticos são "crimes por computador" praticados no espaço cibernético. Os crimes cibernéticos podem ser divididos em dois grupos: stricto sensu e lato sensu. Os crimes cibernéticos lato sensu são os antigos crimes, já tipificados nas leis penais, cometidos utilizando-se o espaço cibernético e ferramentas modernas para a concretização de suas atividades ilícitas. Essas atividades podem ser exploração sexual de menores, ameaças, calúnia e difamação, tráfico de drogas, lavagem de dinheiro, crimes do colarinho branco, danos, fraude, falsificação e outros. Os crimes cibernéticos stricto sensu são os "crimes" que não poderiam ser cometidos sem a utilização do espaço cibernético, como terrorismo cibernético, acesso sem autorização a sistemas de computador, disseminação de programas maliciosos, cyberstalking e outros [1, 2, 3 e 4].

A característica dos crimes cibernéticos que mais dificulta o seu combate é o fato de não existirem fronteiras em sua consecução, podendo a mesma ação criminosa ter efeito em vários países, de forma simultânea, podendo atingir até milhões de pessoas, como é o caso da disseminação de programas maliciosos. Dadas as características dessa ação criminosa, em que muitas vezes as suas provas são perdidas definitivamente em poucos meses ou em poucas semanas, para o seu combate efetivo é necessária a cooperação internacional entre os agentes públicos encarregados deste mister, que deve ser feita por meio de grupos organizados e estruturados em cada um dos países, de forma que tais grupos possam adotar imediatamente todas as medidas necessárias. Também é imprescindível que a Polícia disponha de laboratórios forenses, com todos os equipamentos e softwares necessários, bem como de treinamento para os policiais. Internamente, dentro de cada um dos países, é necessário que haja uma maior proximidade entre a Polícia, o Ministério Público e o Poder Judiciário, de forma a se viabilizar uma maior celeridade nos procedimentos, possibilitando-se que tais criminosos possam ser identificados e punidos.

Uma das características mais marcantes dos crimes cibernéticos é o seu alcance global, podendo a mesma atividade criminosa atingir vários países, de forma simultânea. A natureza global e sem fronteiras do espaço cibernético possibilita que um criminoso cometa uma ação ilícita em um determinado país, de modo a prejudicar milhares de pessoas em diversos países no mundo, causando prejuízos incalculáveis a milhões de pessoas.

Em decorrência do caráter internacional dos crimes cibernéticos, podendo os mesmos

surtirem efeitos em vários países e em milhares de pessoas simultaneamente por todo o mundo, para que seja possível a apuração desses crimes muitas vezes é necessária a cooperação internacional das forças policiais de vários países, de forma organizada e célere. Em função da necessidade de se preservarem os direitos humanos, especialmente com relação à privacidade individual e à inviolabilidade das correspondências, para se garantir o necessário acesso às informações das atividades dos internautas suspeitos de estarem praticando crimes cibernéticos, são necessárias cartas rogatórias do país interessado na apuração dos fatos e ordens judiciais do Poder Judiciário do país em que os dados estão armazenados. Somente após todos esses trâmites burocráticos, que podem demorar longos meses, é que os peritos poderão ter acesso às informações necessárias para a realização das investigações e dos exames, visando à elaboração do laudo. Devido à morosidade desses procedimentos, muitas vezes não é possível a realização dos exames periciais e nem tampouco se chegar à autoria do crime, mesmo com a ordem judicial, visto que os provedores de serviços de Internet dificilmente preservam as informações necessárias por mais de 90 dias [1, 2, 3 e 4].

A perícia em casos de crimes cibernéticos tem como elemento diferencial o fato de que as evidências podem ser perdidas permanentemente, e muitas vezes essa situação fica fora do controle dos peritos. Nesses casos, as informações ficam sob a guarda dos provedores de serviços de Internet, de quem a Perícia fica totalmente dependente. Nos casos de crimes por computador cometidos fora do espaço cibernético, a situação é mais simples, bastando a realização do espelhamento (ou clonagem) das mídias questionadas, preservando-se dessa forma as evidências. A partir dessa etapa, os exames periciais são realizados nas réplicas geradas, evitando-se possíveis adulterações dos dados. Os exames são feitos em consonância com os quesitos formulados e apresentados ao Perito. Várias ferramentas periciais podem ser necessárias, de acordo com as barreiras encontradas durante a realização dos exames. Podem ser encontrados dados encriptados, sistemas protegidos por senhas, dados apagados e outros desafios que devem ser superados pelo Perito.

A preservação das evidências em locais de crimes cibernéticos e demais crimes por computador é de fundamental importância. Quando se tratam de crimes praticados no espaço cibernético, a preservação é bem mais complicada, principalmente quando o provedor de serviço de Internet for estrangeiro. Neste caso há a necessidade de que os Agentes Públicos brasileiros encarregados da apuração do crime façam, por meio de Carta Rogatória, solicitação circunstanciada, comprovando com indícios veementes a ocorrência do crime e a possível autoria, para que tal solicitação seja apreciada pelo Poder Judiciário do país em que o provedor esteja instalado, e que o mesmo tenha elementos para determinar a quebra do sigilo telemático do suspeito. Ressalte-se que, em decorrência do grande volume de dados manipulados e da falta de legislação disciplinando o assunto, os provedores de serviços de internet normalmente preservam os históricos das atividades dos usuários por no máximo até 90 dias. Devido ao acúmulo de trabalho dos órgãos encarregados da apuração dos crimes, esse prazo não é suficiente para a tomada de todas as ações necessárias, o que resulta na quase certeza de impunidade dos infratores [1, 2, 3 e 4].

Cooperação Internacional

Com base na experiência do Serviço de Perícias em Informática (SEPINF) do Departamento de Polícia Federal em investigações de crimes cibernéticos com efeitos em mais de um país, constatamos que, na grande maioria das vezes, tornam-se inócuos todos os esforços empreendidos pelos policiais, em decorrência da morosidade e, às vezes, da impossibilidade de se conseguirem informações armazenadas em provedores de serviços de Internet localizados em outros países. São necessárias Cartas Rogatórias para o afastamento dos sigilos telemáticos que, quando obtidas, as empresas responsáveis pela guarda dos dados (provedores de serviços de Internet) já liberaram as mídias magnéticas para outra finalidade, tendo as evidências sido perdidas definitivamente.

Julio Fernandes

Peritos do Serviço de Pericia em Informática da PF debatem sobre mídias a serem periciadas

Sabe-se que os provedores mantêm as suas cópias com os "logs" dos acessos e demais evidências por períodos bem curtos. Considerando-se a atual forma de trabalho, com a necessidade de Cartas Rogatórias, Ordens Judiciais e demais procedimentos, este prazo não é suficiente, o que inviabiliza todo o trabalho de investigação.

Há vários casos trabalhados por este SEPINF, em que criminosos brasileiros, utilizando-se do espaço cibernético, atacaram sítios de entidades governamentais

estrangeiras, causando sérios danos. Ressalte-se que o Brasil possui os maiores e mais bem estruturados grupos de criminosos cibernéticos (hackers e crackers). Quando o processo chega para este Serviço realizar as perícias, já se passaram meses ou até anos, não havendo como se chegar à autoria do crime, visto que os dados já se perderam definitivamente.

Com o objetivo de tornar eficaz a investigação de crimes cibernéticos, quando a ação criminosa tem origem e/ou efeitos em vários países, fizemos proposta junto à Organização dos Estados Americanos (OEA) e ao grupo "Rede de Emergência 24 horas/7dias", para o estabelecimento de algumas medidas, conforme listado a seguir:

1) Criação de grupos técnicos especializados em todos os países membros da OEA. Sabe-se que já existe a "Rede de Emergência 24 horas/7dias", da qual o DPF faz parte por meio deste SEPINF. Este grupo está estruturado em diversos países e pode ser utilizado.

2) Em casos de incidentes envolvendo possíveis crimes cibernéticos de repercussão internacional, o Grupo Técnico do país prejudicado encaminharia o pedido de cooperação aos Grupos Técnicos dos países envolvidos, com todas as evidências disponíveis, de forma a comprovar a ocorrência do possível crime. Esses pedidos seriam feitos da forma mais rápida, por telefone ou por e-mail, garantindo-se a máxima celeridade.

Julio Fernandes

Policiais são treinados para enfrentar essa nova face do crime

3) Ao receber a solicitação de cooperação, os Grupos Técnicos dos países envolvidos imediatamente iniciariam procedimento investigatório com base nas evidências recebidas. Os próprios responsáveis pela investigação dos países envolvidos, após investigação preliminar e obtenção das necessárias evidências, solicitariam o afastamento do sigilo telemático ao Poder Judiciário de seus respectivos países, dispensando-se, dessa forma, as Cartas Rogatórias e outros procedimentos morosos, visto que os pedidos de afastamento de sigilo seriam feitos com base em investigações feitas dentro do próprio país.

4) Com base nas Ordens Judiciais para o afastamento do sigilo telemático, os policiais obteriam junto aos provedores de serviços de Internet locais todas as informações necessárias para se chegar à autoria dos crimes. Dessa forma, o combate aos crimes cibernéticos dar-se-á de forma eficaz e eficiente, evitando-se as burocracias desnecessárias.

Conclusão

Os crimes cibernéticos e demais crimes por computador estão experimentando um grande crescimento nos últimos anos. Se tais atividades criminosas não forem combatidas com o devido vigor, pode haver grande prejuízo nas atividades sérias que vêm sendo conduzidas por meio do espaço cibernético, tanto as atividades comerciais como as científicas e as governamentais. O combate eficaz dos crimes cibernéticos passa pela cooperação internacional, pela modernização e pelo treinamento da Polícia, preparando os policiais para enfrentarem essa nova face do crime que o século XXI nos apresenta. Passa também pela aproximação da Polícia com o Ministério Público e com o Poder Judiciário, visando à celeridade dos procedimentos. Também são necessárias leis específicas tipificando os crimes cibernéticos, de modo a facilitar o trabalho dos agentes públicos encarregados dessa atividade.

Nos casos em que as atividades criminosas ultrapassam as fronteiras do país, é imprescindível que haja a cooperação internacional, por meio dos grupos de apoio formados pelos órgãos governamentais responsáveis. É importante que esses grupos atuem com eficiência e eficácia, evitando-se maiores burocracias, buscando-se a necessária celeridade exigida por esse tipo de crime. Também é muito importante o apoio das empresas provedoras de serviços de Internet. ■

Bibliografia

1. Council of Europe, "Convention on Cybercrime", Council of Europe - ETS No. 185 - Convention on Cybercrime, Budapest, 23.XI.2001.
2. Paulo Quintiliano da Silva, "Crimes Cibernéticos no Contexto Internacional", Anais do XIII Congresso Mundial de Criminologia, Rio de Janeiro/RJ, 2003.
3. Paulo Quintiliano da Silva, "Perícias em Crimes Cibernéticos", Anais do XVII Congresso Nacional de Criminalística, Londrina-PR, 2003.
4. Zeviar-Geese, Gabriole, "The State of the Law on Cyberjurisdiction and Cybercrime on the Internet", California Pacific School of Law, 2001.

A formação de provas no Ciberespaço

"Considerar como válido apenas o que for recolhido presencialmente, além de inadequado, é incompleto"

As evidências em investigações criminais surgem através de vários meios, nos locais onde haja suspeita de cometimento de delito, atos preparatórios ou conseqüentes, a fim de estabelecer com precisão as circunstâncias do feito

1. Definições para Local

"Espaço. [do latim spatiu].
... Lugar mais ou menos bem delimitado, cuja área pode conter alguma coisa. ...".

"Local. [do latim locale].
... Circunscrito ou limitado a uma região ... Lugar, sítio ou ponto, referido a um fato. ..."

"Lugar. [< latim locale (adj.), 'local'.].
Espaço ocupado; sítio. Sítio ou ponto referido a um fato. Espaço próprio para determinado fim. ..."

"Sítio. [do latim situs, us, 'situação, posição' ?]
... Lugar, local, ponto. Lugar assinalado por acontecimento notável. ..." ( )

2. Estudo de caso

A – Agressores modificam bancos de dados do sistema de nomes de domínio (dns), com aparatos compostos por computadores conectados à Internet, equipamentos acessíveis mediante explorações de falhas de segurança (no popular, invadidos), bem como implementam sítios em provedores de conteúdos.

B – O crime ? Realizar compras, transferências eletrônicas, pagar taxas, impostos, após obter dados sigilosos iludindo o cidadão desatento com a simulação de sítios reais de lojas, instituições financeiras, etc.

A essência desta elaboração se traduz na obtenção de vantagem financeira.

Situando geograficamente o conjunto, cada computador encontra-se em um diferente estado brasileiro, exceto o do provedor de conteúdo que presta seus serviços em outro país. O liame que os deixa a disposição do bando é a grande rede.

3. Sobre o crime

A trama, se comparada aos roubos ou estelionatos convencionais, oferece ínfimos riscos à integridade física dos sujeitos ativos. Suas ações constituem fatos típicos em diversos momentos, desde a criação do aparato para enganar internautas até o momento em que são realizados, por exemplo, os saques das contas-correntes.

Ampliando o exemplo com uma variação destes ilícitos, bastante comum e amplamente divulgada na imprensa nos últimos meses, emprega-se a interceptação de fluxos de dados. Os "sujeitos passivos" são ludibriados com ofertas de crédito facilitado, viagens de férias gratuitas e outros, desde que instalem programas em suas máquinas pessoais. Estes podem ter sido remetidos por mensagens eletrônicas (spam, hoax ...), ou as mensagens sugerem que se faça uma cópia (download) de arquivos contidos em sítios diversos. Muito curiosos são os casos em que as ofertas tratam da possibilidade de participar em programas de TV que oferecem prêmios ou os ditos reality shows.

4. Lugar do crime

Sem mais, qualquer ponto no mapa de nosso território onde se coloque um marcador apontando computadores do exemplo, seja do bando, do provedor ou dos usuários, será corretamente visto como lugar, bem como no estrangeiro enquanto crime a distância pois "a ação ou omissão se dá em um país e o resultado ocorre em outro".

5. O Tempo do crime

Ainda sobre o exemplo, suponhamos que aconteça uma primeira transferência bem-sucedida, por parte dos criminosos, de valores. Constatada a capacidade técnica e o bom funcionamento do ardil, difícil é estabelecer um fim quando as oportunidades parecem ser tantas, sobretudo imaginando quem poderia desvendar as faces que observam as telas.

Continuando o sítio falso "no ar", tantos outros inocentes repetem os gestos descuidados que a quantidade de informações interceptada espanta os receptadores, trabalhando em ritmo intenso para selecionar contas úteis. Quase em paralelo são movimentados valores, de tal maneira espalhados e fragmentados que o rastreamento não pode ser feito de imediato.

As atividades delituosas, por acontecerem em diversos momentos e muitas concomitantemente, por vezes geram confusão sobre quais seriam as ações preparatórias, de execução, de produção dos resultados, se coligadas ao mesmo crime que continua acontecendo ou se pertencentes à outro cometido em seqüência.

O problema pode ser resolvido a partir da observação precisa de cada tipo penal, juntando ocorrências relacionadas, verificando sistematicamente a satisfação de premissas e encadeando com propriedade os eventos.

6. Provas - possibilidades e certezas

Em se tratando de crimes essencialmente materiais, a formação de provas se dará mediante juntada de vestígios em número suficiente, desde que cada qual acrescente algo em termos de probabilidade de ocorrência de fatos concretos. Não basta apenas localizar uma chave-defenda no jardim adjacente à residência que foi furtada. É preciso que haja alguma marca passível de ter sido produzida por pressão da ferramenta para ocasionar o arrombamento da porta da cozinha.

Julio Fernandes

Celulares e agendas eletrônicas podem ser utilizados para cometer crimes na área de informática

Usando outros termos, um número reduzido de linhas de registros de eventos (logs) consideradas de forma isolada, mesmo que representem adequadamente um padrão conhecido de exploração de vulnerabilidade, pode ser de pouco interesse. Se, por exemplo, for adicionada a hora de criação de um arquivo com código executável, de sugestivo nome "intercep", com um arquivo de senhas, modificado após alguns instantes, pode-se progredir consistentemente na concatenação e construção do iter.

7. Objetivos da perícia em local de crime

De acordo com o Princípio da Transferência de Locard "ocorre transferência mútua de vestígios quando existe contato entre dois objetos ou duas pessoas, o que implica que haja provas/vestígios em todos os locais em que são cometidos crimes. Os autores podem deixar ou retirar provas/ vestígios no local, bem como aqueles que os recolhem." ,

Importante mesmo é tentar perceber as perturbações provocadas no mundo externo causadas por ação de pessoas ou da natureza, como uma cadeira fora do lugar, uma mancha de sangue ou um registro de acesso em computador.

Por estarem próximos os elementos podem completar um quadro maior, a exemplo da escrita a tinta no monitor com a inscrição "type_0", relacionada com os dados armazenados na memória do computador. Não obstante, vários locais estarão se interligando como nos exemplos anteriores, cabendo ao examinador compreendê-los de maneira adequada.

Quando da existência de diversos locais como acima, o recolhimento de vestígios de proveniências diversas ocorre com o objetivo de aumentar o grau de certeza sobre os eventos, seu(s) autor(es), conseqüências, tempo, seqüência dos fatos, etc. Em princípio, não existe hierarquia entre os locais e sua relevância está diretamente relacionada a quantidade ou qualidade do que neles for encontrado.

Julio Fernandes

As CPUS dos computadores também são periciadas

Julio Fernandes

HDs, CDs, disquetes são mídias examinadas pelos peritos

8. A observação dos locais

Os métodos de busca podem variar de acordo com as circunstâncias, sendo exemplos o percorrimento de áreas em espiral, grelha, faixa, zona ou roda. O posicionamento dos vestígios costuma ser relevante, daí o destaque para "esquemas elucidativos" no nosso C.P.P., bem como o emprego de fotografias, filmes, diagramas, plantas ou a apresentação da topologia de uma rede de dados.

São exemplos de pormenores significativos(4) nos locais convencionais

- Condições meteorológicas (chuva, sol, vento);
- Pontos de acesso, como portas e janelas (abertas ou fechadas);
- Odores (perfume, fumo,óleo, gás);
- Feridos/sua posição/ferimentos visíveis/vestuário;
- Mortos/sua posição/ferimentos/rigor mortis/hipostase (acumulação do sangue após a morte);
- Objetos usados para ferir;
- Peças de vestuário;
- Roupa de cama, com eventuais fluídos corporais;
- Pelos humanos;
- Micro-vestígios de origem humana;
- Impressões digitais;
- Marcas - pés, sapatos, etc;
- Material audiovisual;
- Agendas, anotações;
- Ferramental de apoio ao crime - chave-de-fenda, pé-de-cabra, etc.

Tratando especificamente de material informático

- CPU ;
- Monitor ;
- Teclado;
- Impressora;
- Papel de impressora;
- Material Impresso;
- Modem;
- Discos óticos;
- Disquetes;
- Discos rígidos;
- Fitas magnéticas;
- Gravadores de CD;
- Placas de circuitos eletrônicos;
- Cabos de comunicação;
- Manuais técnicos;
- Memórias avulsas - memory sticks, compact flash, memórias com conexão usb, etc.

Estas amostras são como o grão de areia em uma praia, sendo possível destacar inúmeras outras suscetíveis à inspeção. Mesmo que cada objeto esteja sujeito ao escrutínio segundo regras específicas de cada corpo do conhecimento científico, o trabalho do perito segue diretrizes genéricas como a ação planejada e metódica, a preocupação em preservar evidências, o cuidado com cada minúcia e a atenção ao detalhe.

9. O ciberespaço

A infra-estrutura que sustenta o dito ciberespaço, resumida hoje através da implementação da rede que interliga redes – a Internet – é composta por um amalgama de tecnologias, pessoas, entidades de ensino, universidades, empresas, governos e organismos não-governamentais, em uma disposição colaborativa bastante singular, pois acontece por iniciativa das partes que descobriram nesta forma de comunicação inúmeras utilidades.

Tratando de alguns conceitos ligados à tecnologia temos

A – PROTOCOLOS

Compõe a linguagem que as máquinas compreendem e através deles se comunicam, desde computadores localizados no Japão aos situados em nosso território;

B – SERVIÇOS

Disponíveis para execução de tarefas como comunicação interativa (chat), publicação de conteúdos em páginas e sítios, transferências de dados, tramitação de correspondência eletrônica e outros;

C – ENDEREÇOS DE IP

Cada computador ligado à Internet deve possuir um endereço com características únicas, capaz de identificá-lo em meio aos

demais e tornar possível o envio e recebimento de dados a ele direcionado. No dialeto dos equipamentos eletrônicos, os endereços são formados por seqüências numéricas por vezes comparadas com o conceito do número de terminal telefônico;

D – SUB-REDES

Endereços de IP são distribuídos ao redor do planeta de forma peculiar, sendo cada fatia, chamada como sub-rede, atribuída a um ente, que poderá repartir ainda mais a parte que lhe cabe. Cada sub-rede está sob controle de um organismo, podendo este realizar novas divisões repassando o controle a terceiros. Sendo assim, a um endereço estão associadas informações sobre empresas, governos ou organismos não-governamentais, que podem ser obtidas por meio de pesquisas na Internet;

E – ROTAS

O IP, ou protocolo entre redes (internet protocol), sobressaiu-se em parte devido à robustez que oferece ao conjunto, pois oferece alternativas dinâmicas para o fluxo de dados, desviando a comunicação de um nó falho da rede toda vez que houver um caminho alternativo, sem prejuízos para comunicação entre os demais;

F – A IDENTIFICAÇÃO DE CONTEÚDOS E SERVIÇOS AGRUPADOS EM DOMÍNIOS

Ao ser humano nunca foi tarefa palatável identificar equipamentos puramente através de números, sendo utilizado desde os primórdios da Internet alguma forma de correlacionar números com nomes, culminando com o estabelecimento em 1984 do Domain Name System, ou Sistema de Nomes de Domínios .

Repetindo a síntese tão apropriada de Jon Postel, "Um nome indica o que procurar. Um endereço aponta aonde encontrar. A rota diz como chegar até lá." ( ).

10. Em Busca de Vestígios em Materiais de Informática

Em diversas situações os crimes cometidos com o emprego do material de informática como instrumento são categorizados como crimes virtuais. Nada mais impróprio.

É certo que os computares armazenam representações digitais de conceitos, idéias ou objetos do nosso mundo. Pois justamente estas, para que sejam depositadas em mídias, necessitam que coisas como magnetização de superfícies metálicas ou feixes de laser modificando substratos orgânicos aconteçam. A comunicação de dados, por sua vez, é feita através da transmissão de ondas eletromagnéticas. Os processos de armazenagem e transmissão se realizam através de fenômenos físicos observáveis e com existência clara em nosso mundo. Vale lembrar, porém, que estes têm como característica a volatilidade no tempo.

Em tempos recentes a abordagem dos locais trazia a recomendação quase unânime de desligar as máquinas prontamente. Hoje, há que se levar em conta a possibilidade de um invasor ser bem preparado, cuidando para trabalhar apenas com a memória volátil, ou seja, sem gravar dados em áreas permanentes como arquivos em disco. Considerando o grande volume de memória em equipamentos atuais, assim provavelmente procede o criminoso.

Frutos de experiências práticas, com vistas à obtenção de melhores resultados, surgiram categorizações de elementos de acordo com sua volatilidade. Assim são enumerados os itens abaixo, onde primeiro constam aqueles mais voláteis seguidos dos que têm maiores chances de permanecer intactos mais tempo:

I – Registros de processador e memória cache

II – Memória principal

III – Estado das conexões de rede

IV – Estado dos processos em execução

V – Conteúdo das mídias não-removíveis

VI – Conteúdo das mídias removíveis.

Esta classificação considera o emprego costumeiro de cada elemento, existindo situações onde diversos fatores contribuem para alteração desta ordem e que demandam tratamentos diferenciados.

Sendo assim, as atitudes iniciais do perito devem tentar resguardar aquilo que tem maiores chances de se esvair, lembrando que em situações reais o melhor dos procedimentos pode ser insuficiente.

A fim de manter a coesão dos exames o perito tem que observar seus atos, registrando-os e conhecendo todas as suas implicações.

Assim como a observação de um fenômeno interfere neste, lembrando ainda o Princípio da Transferência de Locard, o processo de análise de sistemas informatizados que estejam em funcionamento produz alterações de estados. Na tentativa de reproduzir conteúdos da memória principal ou de memórias auxiliares é necessária a execução de comandos, sobrescrevendo áreas daquela. Por outra via, ao desligar o equipamento perde-se o conteúdo de suas memórias voláteis.

São inúmeros os casos concretos onde saber fazer escolhas, sobre "aquilo que pode ser salvo e preservado" para futuro escrutínio da criminalística, é o melhor que o perito tem a oferecer.

Basta lembrar quantas atividades comerciais não podem ser interrompidas, sob risco de provocar sérios prejuízos ao negócio. Como proceder quando estas devem ser examinadas? Por vezes ainda há que se fazer algo para suprir a falta de recursos que impedem o pronto atendimento, não restando alternativa além de uma longa espera até o momento em que policiais compareçam fisicamente ao lugar.

11. Os Locais no Ciberespaço

Em diferentes momentos os peritos conduzem a obtenção de vestígios. No exemplo acima a seqüência poderia ser:

1 – Chegada aos olhos e ouvidos dos peritos do alerta. A notícia-crime traz fatos ao conhecimento dos auxiliares da justiça, como a existência de sítio falso de instituição bancária, o desvio inusitado e ainda não bem compreendido do fluxo de dados para este ambiente, bem como a constatação de transferências indevidas de valores de contas-correntes de vítimas;

2 – Os peritos procuram mais dados sobre o sítio: possui nome registrado (como www.sitiofalso.com.br); é apenas referendado por endereço numérico (endereço IP); os responsáveis pela infra-estrutura em que funciona; quais os caminhos ou por quais sub-redes seguem os fluxos de dados até atingi-lo; demais vestígios que se apresentem. Todos estes dados são obtidos, quase que exclusivamente, junto à Internet e, portanto, disponíveis em qualquer ponto interconectado do planeta;

3 – As constatações conduzem à diversas ramificações em etapas investigativas conseqüentes;

4 – Ciclo de exames em locais - juntada de vestígios - exames em laboratórios;

5 – Consolidação de vestígios recolhidos ao longo do apuratório em laudo.

O texto do C.P.P. comanda, com muita propriedade, que "... não se altere o estado das coisas até a chegada dos peritos...". Ao Estado portanto compete prover estrutura e condições de trabalho para seus órgãos de criminalística, tornando factível a execução dos preceitos legais.

A disseminação da conectividade traz a reboque a distribuição de recursos, possibilitando a utilização de serviços computacionais a despeito de sua localização física. Muito embora a volatilidade dos meios digitais, conjugada com a dispersão geográfica dos sítios, exija maior agilidade, simultaneamente a tecnologia traz facilitadores, pois permite que os lugares sejam alcançados à distância.

Se um sistema é acessado indevidamente e o seu administrador, ao fazer uma notificação às autoridades, precisa de imediato tomar atitudes que visem corrigir falhas de segurança e reconfigurar as proteções do ambiente, o socorro pode ser feito remotamente, via Internet, concomitante ao recolhimento de vestígios.

Considerar como válido apenas o que for recolhido presencialmente, além de inadequado, é incompleto.

Muitos autores apresentam indicações, sempre observando a consideração antecipada dos fatores positivos e negativos de qualquer linha de conduta. Podem ser citadas:

- Planejar o trabalho antecipadamente;
- Agir metodicamente, registrando tudo o que for realizado;
- Minimizar alterações decorrentes da coleta de vestígios, como ao evitar mudanças em datas de arquivos, diretórios e áreas relevantes de mídias;
- Iniciar o processo de inspeção pelos itens mais voláteis.

Existem diversas ferramentas de análise, que possibilitam recuperar o que seria desperdiçado de outra forma. Alguns sistemas operacionais dispõem de utilitários para verificar programas em execução, conexões de rede ativas ou usuários conectados .

Se uma seqüência de passos for corretamente pensada, é possível até realizar imagens remotas de mídias ou analisar efeitos de artefatos enquanto em execução.

Um bom exemplo de pontos a serem considerados quando do recebimento de uma notificação de incidente seria :

a) Quando se imagina que ocorreu;

b) Como foi detectado;

c) Quando foi detectado;

d) Conseqüências que a pessoa observa e as imaginadas para o futuro;

e) Sobre o equipamento comprometido:
I – hardware/software/sistema operacional envolvido;
II – descrição da rede: topologia, endereçamento, etc;
III – função da máquina na rede;
IV – presença de documentos importantes;
V – localização física;
VI – segurança física;
VII – usuário principal e administrador do equipamento;
VIII – status corrente do equipamento;

f) Ações realizadas pelo agressor:
I – atividade em curso?
II – endereço de origem identificado?
III– código malicioso inserido?
IV– trata-se de negação de serviço?
V – apenas vandalismo?
VI– existem pistas sobre possível ação

interna ou externa?

g) Ações realizadas pelo usuário:
I – feita desconexão do equipamento?
II – foram examinados registros de acesso (logs)?
III– é possível acesso remoto ou local?
IV– foram percebidas alterações em outros equipamentos da rede?

h) Ferramentas disponíveis no equipamento :
I – ferramentas específicas de auditoria;
II – monitores de rede.

Alguns programas orientados para inspeção de sistemas podem também ser utilizados, oferecendo rotinas extensas de análise e relatórios com resultados consolidados:

Comandos "ping", "traceroute", "host", pacotes como o "Strobe", "Grabbb", "Nmap", "Nessus": a ação de "mapeamento" de uma rede permite identificar sua topologia, equipamentos servidores, sistemas operacionais, serviços de rede em funcionamento e suas versões, etc;

Pacotes como "tcpdump", "ngrep", "Snort", que servem à detecção de intrusos, são fonte vastíssima para revelação de padrões de ataques;

É possível realizar exames nos sistemas enquanto estiver funcionando, mediante o franqueamento do acesso, permitindo listar processos em execução, conexões de rede ativas, usuários conectados, ou mesmo fazer a duplicação de dados de partições;

Ferramentas típicas de agressores, os "sniffers" são essenciais para monitorar e observar o que acontece em uma rede de dados.

Sites como o de apologia ao racismo (acima) são exemplos de crimes cibernéticos

Sobre a interceptação de fluxos de dados, embora muitos vejam apenas como mais um tipo de "grampo", merece que seja feita uma ressalva. A sua execução permite inspecionar algo mais que relatos, opiniões, desejos e impressões, como aquilo que se vê em conversações telefônicas. De fato, constata-se também a transmissão de comandos que resultam em alterações de estados em outros equipamentos e sistemas, servindo como indícios para comprovar coisas como o desligamento de uma máquina, a deterioração de um serviço, a mudança do conteúdo de um arquivo ou a introdução de código malicioso em um computador.

12. Conclusão

O exposto compõe parte do contexto com o qual se deparam os auxiliares da justiça na exploração do ciberespaço.

Observações com a do Dr. Ricardo Pereira, dizendo que "... é de concluir-se que o uso da Internet tornou-se um fato jurídico, do qual nascem, subsistem e se extinguem relações jurídicas.", podem ser complementadas notando que, em muitos casos, somente pelo acesso direto à Internet estas relações são observáveis. Destarte, dita a Constituição Federal em seu art. 5 - XXXV "...a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito;...".

O Código Processual Civil estabelece em seu art. 332 que podem ser admitidos como prova "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.".

Portanto, é certo que as redes de computadores podem oferecer vestígios quando da busca da verdade, não sendo estes vislumbrados senão mediante inspeção direta daquelas. ■

A perícia ensina

A APCF promove cursos, palestras e seminários. O objetivo é mostrar e provar para a sociedade que é possível ajudar a combater a impunidade no país. Se sua entidade ou empresa quer saber mais sobre a Perícia Criminal, venha conhecer as palestras ministradas por experientes peritos criminais:

MÓDULOS / SEQÜÊNCIA

- Introdução à Criminalística
- Legislação Processual Pericial
- Local de Crime
- Obras superfaturadas
- Caça-níqueis
- Cocaína, seu DNA e suas Cores
- Crimes de Trânsito
- Meio Ambiente
- Perícias de Laboratório
- Balística Forense
- Vistoria de Identificação Veicular
- Documentoscopia
- Fonética Forense
- Crimes de Informática
- Crimes Financeiros - Lavagem de dinheiro

Educar para conscientizar

APCF

Associação Nacional
dos Peritos Criminais Federais

A APCF é a associação que congrega os integrantes do cargo de perito criminal federal do Departamento de Polícia Federal

Paternidade. Uma questão de confiança.

Curso Paternidade e Identificação Humana (HID)
de 23 à 26 de novembro de 2004

Dr. Rinaldo Wellerson Pereira
pós-graduação em ciências genômicas
e biotecnologia - UCB

Alexandre Wang, M.Sc.
Senior Field Applications Specialist - Applied
Biosystems do Brasil

informações e inscrições:
abi-expert@appliedbiosystems.com
0800.704 9004 (outras localidades)
5070.9662 (Grande SP)

"Com o aumento da demanda dos testes de paternidade por DNA, tornou-se necessária a utilização de técnicas mais rápidas e confiáveis. O uso de instrumentos automatizados e kits de reagentes, ambos validados para a investigação de paternidade, facilita e agiliza a rotina do laboratório aumentando a produtividade e confiança no resultado. A Applied Biosystems é a única empresa a oferecer uma solução completa para o laboratório de paternidade incluindo instrumentos de análise, softwares específicos, kits de reagentes, treinamento e suporte científico."

Para maiores informações acesse: **www.appliedbiosystems.com/HID**

iScience. Para melhor entender a complexa interação dos sistemas biológicos, cientistas da vida estão desenvolvendo abordagens revolucionárias para descobrir como unir tecnologia, informática e os tradicionais laboratórios de pesquisa. Em parceria com seus clientes, a Applied Biosystems proporciona produtos inovadores, serviços e conhecimentos que fazem com que essa nova **Ciência Integrada** seja possível.

Applied Biosystems