SEGURANÇA DO INTERNET BANKING NO BRASIL[1]

Rafael Vaz Gallao[2]
Alberto Martins Junior (Orientador)[3]

RESUMO

Este artigo apresenta uma pesquisa realizada sobre a história e o funcionamento do serviço de *Internet Banking* no Brasil desde sua criação. O artigo analisa dois tipos de ataques contra o serviço de *Internet Banking*, o roubo ou furto de senhas e o ataque aos servidores de nomes conhecidos como DNS. O roubo ou furto de senha pode ser realizado de várias formas, uma delas é a utilização de programas que analisam o tráfego de dados em uma rede e seleciona as informações relativas à login e senhas de usuários, assim os criminosos podem obter informações, como por exemplo, os *logins* e senhas, e usar as informações para desviar quantias de dinheiro de maneira criminosa. Outra forma de realizar roubo ou furto de senhas que será comentada neste artigo é a utilização de engenharia social, que é basicamente o ato de enganar pessoas, usuários ou clientes para se conseguir vantagens, o que a lei chama de estelionato.
Outro método de ataque ao serviço de *Internet Banking* que será comentado neste artigo é o ataque sobre o servidor de nomes, o DNS. Estes ataques normalmente são feitos por criminosos que tentam responder com informação erradas as requisições de uma resolução de nome que um cliente faz a um servidor DNS. Um site de banco falso também pode ser usado no ataque, no momento em que o usuário utiliza o site falso o criminoso comete o ataque, pois sites falsos podem conter inúmeras armadilhas para o usuário.
Além das abordagens sobre os ataques descritos acima, também serão comentadas as defesas para estes ataques e também quem são os principais alvos destes ataques na Internet.

Palavras-chave: Redes ; *Internet Banking ;* Segurança

ABSTRACT

This paper presents a research on the history and workings of the *Internet Banking* service in Brazil since its inception. The paper also examines two types of attacks against the *Internet Banking* service, robbery or theft of passwords and the attack on name servers known as DNS. Theft or stolen password can be accomplished in several ways, one of them is the use of programs that analyze the data traffic on a network and selects the information for login and passwords, so the criminals can obtain information such as logins and passwords, and use the information to divert sums of money in a criminal manner. Another way to accomplish or theft of passwords which will be discussed in this work is the use of social engineering, which is basically the act of deceiving people, users or customers to get benefits, is what the law calls for embezzlement. Another method of attack on *Internet Banking* service which will be mentioned in this work is the attack on the DNS name server. These attacks are usually done by criminals who try to respond with the wrong information to request a name resolution that a client makes a DNS server. A fake bank site is also used in the attack, when the user uses the fake site commits the criminal attack, because this fake site may contain numerous traps for the user.
Besides the approaches of the attacks described above, will also be discussed defenses to these attacks and also who are the main targets of these attacks on the Internet.

Keywords: Networks ; *Internet Banking ;* Security

[1] Artigo Baseado em Trabalho de Conclusão de Curso (TCC) desenvolvido em cumprimento a exigência curricular do Curso Superior de Tecnologia em Analise de Sistemas e Tecnologia da Informação depositado no 1°semestre de 2011.
[2] Tecnólogo em Analise de Sistemas e Tecnologia da Informação - Fatec Americana - Centro Estadual de Educação Tecnológica Paula Souza; Contato leafarvaz@hotmail.com
[3] Prof. Me. Fatec - AM - Graduação em Processamento de Dados, Mestre em Administração de empresas ; Contato: amartins@unimep.br

1 INTRODUÇÃO

Este artigo foca a evolução da segurança para utilização do *Internet Banking*. Foram analisados dados estatísticos sobre alguns tipos de ataques, além dos impactos causados e seus principais alvos.

Os crimes cibernéticos praticados contra o serviço de *Internet Banking* no Brasil é para os especialistas o mais comum, já que na maioria dos casos os ataques visa diretamente o crime de roubo, de acordo com o Desembargador Federal Mario Cesar Ribeiro com base na lei n. 7.716/89, art. 20 infração penal (TRF1, 2001).

Justifica-se a escolha do trabalho devido ao aumento do uso de equipamentos eletrônicos com acesso a Internet no Brasil e conseqüentemente o uso do *Internet Banking*, conforme dados publicados pelo governo federal brasileiro.

> "A posse de computador teve o seu maior crescimento nos últimos cinco anos, de acordo com os mais recentes dados da Pesquisa TIC Domicílios. Em 2009, 36% dos domicílios possuíam computador, enquanto apenas 28% tinham o equipamento em 2008. O mesmo ocorreu com o uso da Internet cujo acesso do domicílio subiu de 20% para 27%, o que representou um crescimento de 35% no período." (Centro de estudos sobre as Tecnologias da Informação e da Comunicação - TIC, 2009)

Com o aumento dos acessos à Internet é provável que mais vulnerabilidades de segurança sejam identificadas e serviços como o *Internet Banking* sejam cada vez mais alvo de ataques. Para entender melhor estas probabilidades é necessário pesquisar e analisar dados sobre a evolução e os ataques praticados contra o serviço de *Internet Banking* no Brasil, com o propósito de melhorar o conhecimento sobre o tema.

Um fato importante e que cada vez mais possível observar é a demanda na utilização das instituições bancárias pela sociedade brasileira. De acordo com a matéria do jornal O Globo (2005) o número de contas correntes bancárias no Brasil elevou-se 37% entre os anos de 2001 a 2006. Em decorrência, as ferramentas bancárias como caixas eletrônicos, serviços de transferência de valores monetários e o serviço de *Internet Banking* também sofreram aumento em sua utilização.

Com o crescimento do consumo dos serviços bancários, as fraudes e crimes aumentam também, principalmente os crimes cibernéticos. Em uma reportagem feita pelo jornal O Globo (2005): um estudo feito entre 14 países colocou o Brasil como o país em que os usuários menos atualizam seus softwares de defesa contra ataques cibernéticos, fato que intensifica ainda mais a prática de crimes envolvendo o serviço *Internet Banking* no Brasil, já que o ponto fraco a ser atacado é o próprio usuário, neste caso o cliente bancário.

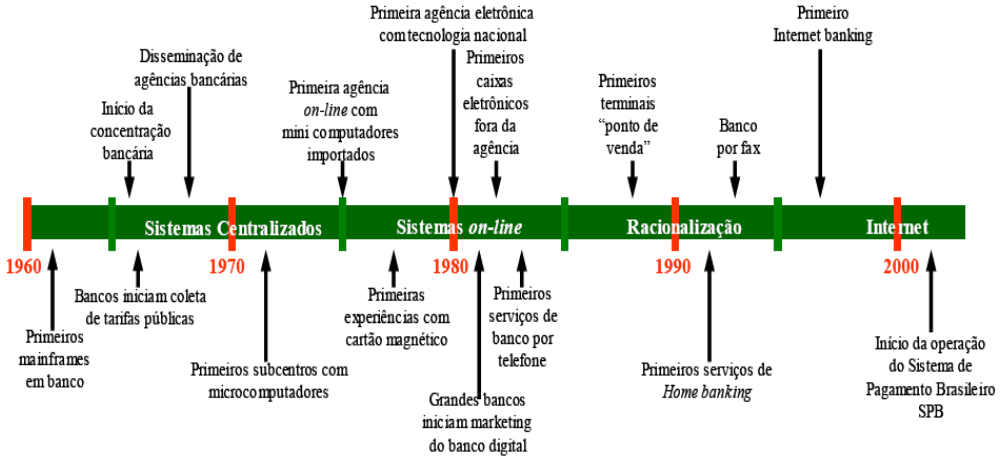
Devido aos fatos descritos acima se justifica a análise da evolução da segurança do serviço de *Internet Banking* no Brasil para entender melhor como os ataques evoluem e como a sociedade brasileira está se preparando para utilização segura do serviço de *Internet Banking* e também como irá punir os criminosos que praticam estes crimes cibernéticos.

2 *INTERNET BANKING*

As instituições bancárias brasileiras vêm investindo cada vez mais em tecnologia para aumentar seus produtos e conseqüentemente mais serviços aos clientes. O *Internet Banking* é um dos serviços que mais tem avançado em sua tecnologia no Brasil (D'ANDRÉA, 2000).

Para Diniz (2003) os bancos têm se desenvolvido ao longo dos tempos, principalmente as tecnologias descobertas após 1965, além da reforma bancária, lei 4.595/64. A partir destas mudanças na década de 70 os bancos tiveram um desenvolvimento "caseiro". Além disso, o autor destaca que os bancos tiveram importante papel para o desenvolvimento do país na década de 70. Durante a década de 80, devido aos problemas com a inflação que ocorriam no país, que modificavam de maneira constante preços e taxas os bancos foram forçados mais uma vez a investir em tecnologia. É possível visualizar essa evolução do sistema bancário brasileiro observando a linha temporal ilustrada na figura 1 (DINIZ, 2004.).

Figura 1: Fases da automação bancária no Brasil



Fonte: *Internet Banking* sob a Ótica da Funcionalidade, Confiabilidade e Usabilidade (DINIZ, 2004).

Com o evento da economia digital (TAPSCOTT, 1997) foi possível a criação de um serviço chamado *Internet Banking*. O Brasil foi um dos países pioneiros na utilização do serviço. O Bradesco, um dos maiores bancos privados do Brasil, foi um dos primeiros bancos no mundo a fornecer o serviço de *Internet Banking* para seus clientes, em 1996 (GATES, 1999). Sucessivamente outros bancos principalmente os de varejo adotaram o *Internet Banking*.

O serviço de *Internet Banking* é como uma nova modalidade de comércio eletrônico, onde o cliente, utilizando a Internet faz acesso a vários serviços bancários, realizando negócios e contratos eletrônicos (GOMES, 2003).

O serviço de *Internet Banking* é no Brasil oferecido aos clientes de três formas segundo Ramos (2000):

> "[...] (1) pela Internet, com acesso através do endereço do banco por intermédio de um provedor de Internet (particular ou gratuito) e com o auxílio de um navegador (*browser*); (2) via aplicativo existente nos sistemas operacionais da *Microsoft Windows*, a rede *dial-up* que, corretamente configurada, permite o acesso sem a necessidade de um provedor; e (3) por EDI, exclusivamente para empresas de grande porte e de volume de negócios compatível com a necessidade da sua instalação."

O termo *browser* faz referência a um aplicativo que permite ao usuário acessar informações em servidores. Estas informações geralmente são hospedadas no formato *Hyper Text Markup Language* (HTML) uma linguagem de computador muito utilizada para construir sites. Já o termo rede *dial-up* é um tipo de acesso à Internet no qual o cliente utiliza um modem e uma linha telefônica para o acesso. Segundo o site www.dip.co.uk o termo *Electronic Data Interchange* (EDI) significa troca estruturada de dados através de uma rede de dados qualquer.

O serviço de *Internet Banking* possui algumas vantagens que justificam o seu investimento, segundo Ramos (2000), como:

> "[...] descongestionar o atendimento, minimizando ao máximo a ida do cliente às agências; reduzir custos operacionais; associar a imagem de banco moderno e automatizado; e aumentar a receita de tarifa, que é repassada integralmente para as agências. Os requisitos apontados também como vantagens pelo banco são: agilidade, conveniência, privacidade (pela não interveniência humana de terceiros) e segurança, desde que sejam observados os padrões de segurança aplicados ao sistema bancário. Outro aspecto é a possibilidade de realizar várias operações em um mesmo ambiente, pela simplificação e integração."

Devido a estas vantagens no serviço de *Internet Banking* sua utilização vem aumentando continuamente no Brasil segundo uma pesquisa realizada pela empresa e-bit (2003). Uma das diretoras da empresa, Fabiana Curi Yazbek informou que o setor bancário no Brasil é um dos mais modernos do mundo e isso auxiliou para o desenvolvimento do *Internet Banking* no país. Hoje um dos maiores bancos nacionais é o que possui mais clientes cadastrados para utilizar o serviço.

A facilidade de compra de computadores e o aumento na utilização da Internet afetam diretamente o uso do *Internet Banking.* Em dados da pesquisa em Tecnologias da Informação e da Comunicação (TIC)

realizada por CGI. BR (2009) abaixo é possível observar melhor este aumento utilizando a tabela 1 e a figura 2.

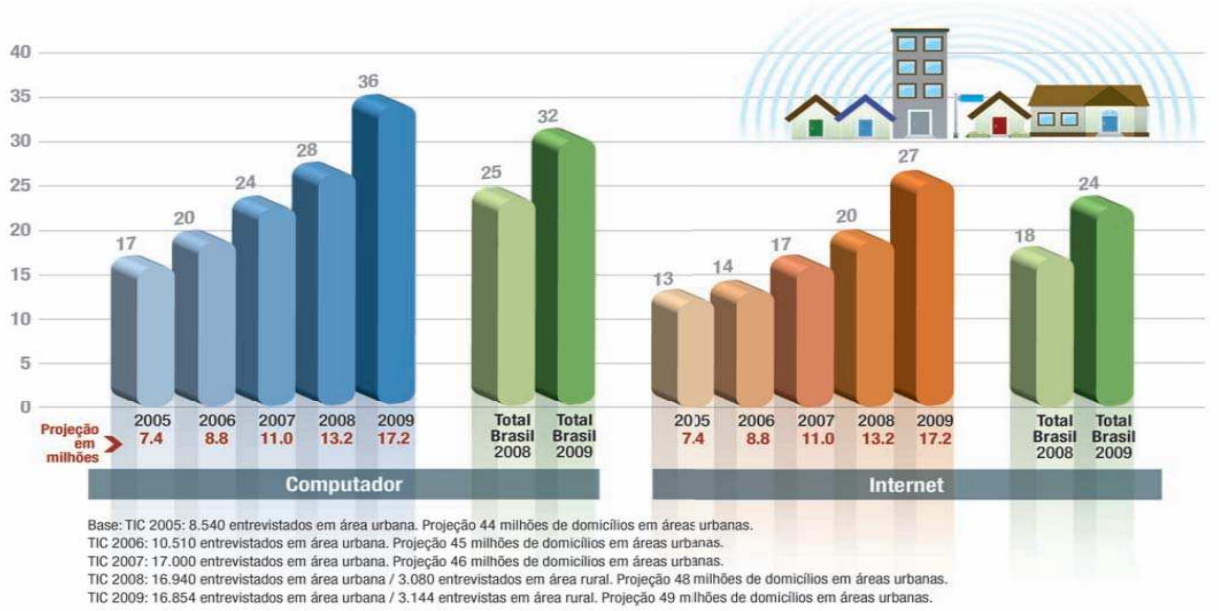
Tabela 1:. Número de usuários de Internet no Brasil, entre 2000 e 2009.

Ano	População total do Brasil (em milhões)	População com acesso à Internet (em %)	População com acesso à Internet (em milhões)*
2000	169,8	5,7	9,8
2001	173,8	6,9	12
2002	176,3	7,8	13,9
2003	178,9	7,9	14,3
2004	181,5	10	19,3
2005	184,1	17	32,1
2006	186,7	18	35,3
2007	188	23	44,9
2008	189,9	28	53,9
2009	191,5	32	63

Fonte: Dados do IBGE (Censo e PNAD) e da Mídia Dados (2000 a 2004). A partir de 2006 os dados são da pesquisa TIC domicílios do NIC. Br.

Na tabela 1 fica nítido o aumento do uso da Internet no Brasil, mesmo se levarmos em conta que a população brasileira teve um crescimento em milhões de 12,7 % durante os anos de 2000 a 2009, assim como o crescimento da Internet para este mesmo período foi de 642,8 %. Os números impressionam, porém se analisarmos os dados de 2009 aproximadamente um terço possui acesso à Internet, ou seja, pode se esperar grande crescimento do acesso no Brasil para os próximos anos. A figura 2 reforça ainda mais esta tendência de crescimento.

Figura 2: Computador e Internet: posse (%)



Fonte: Dados da pesquisa TIC domicílios retirada do site www.nic.br (2009).

Essa maior utilização do serviço pela rede implica em aumento na vulnerabilidade. A integração das organizações por meio da rede de computadores, na qual a sociedade se comunica, através da *web*, do protocolo TCP/IP e de *e-mail*, as expõem em falhas de segurança das informações (GARFINKEL;

SPAFFORD, 1997). O Tribunal de Contas da União (2003), em seu guia de "Boas práticas em segurança da informação", afirma o aumento da vulnerabilidade:

> "Com a chegada dos computadores pessoais e das redes de computadores que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha complexidade que há a necessidade de desenvolvimento de equipes e métodos de segurança cada vez mais sofisticados. Paralelamente, os sistemas de informação também adquiriram importância vital para a sobrevivência da maioria das organizações modernas, já que, sem computadores e redes de comunicação, a prestação de serviços de informação pode se tornar inviável." (TRIBUNAL DE CONTAS DA UNIÃO, 2003).

O crescimento e o aumento do uso do serviço *Internet Banking* motivaram os bancos a se preocuparem com a segurança eletrônica. Para um melhor entendimento deste cenário os próximos capítulos irão analisar alguns tipos de ataques mais comuns contra o serviço de *Internet Banking*, porém antes a apresentação de um capítulo de nivelamento técnico para melhor entendimento destes tipos de ataques e suas defesas.

Para uma melhor interpretação dos principais tipos de ataques e defesas contra o serviço de *Internet Banking* é necessário um conhecimento técnico sobre alguns termos como Internet, DNS, HTTP e o SSL.

2.1 Internet

Os computadores e o crescimento da utilização da Internet afetaram a vida de milhões de pessoas no mundo, causando mudanças significativas no desenvolvimento de algumas atividades. "A rede Internet é a grande responsável pela revolução no mundo das comunicações e dos computadores." (ZANIOLO, 2007). Para mostrar o número de pessoas que utilizam a Internet no mundo, principalmente no Brasil, segue abaixo a ordem de classificação de usuários na tabela 2.

Tabela 2. Top 20 countries with the highest number of internet users.

TOP 20 COUNTRIES WITH HIGHEST NUMBER OF INTERNET USERS - JUNE 30, 2012						
#	Country or Region	Population, 2012 Est	Internet Users Year 2000	Internet Users Latest Data	Penetration (% Population)	Users % World
1	China	1,343,239,923	22,500,000	538,000,000	40.1 %	22.4 %
2	United States	313,847,465	95,354,000	245,203,319	78.1 %	10.2 %
3	India	1,205,073,612	5,000,000	137,000,000	11.4 %	5.7 %
4	Japan	127,368,088	47,080,000	101,228,736	79.5 %	4.2 %
5	Brazil	193,946,886	5,000,000	88,494,756	45.6 %	3.7 %
6	Russia	142,517,670	3,100,000	67,982,547	47.7 %	2.8 %
7	Germany	81,305,856	24,000,000	67,483,860	83.0 %	2.8 %
8	Indonesia	248,645,008	2,000,000	55,000,000	22.1 %	2.3 %
9	United Kingdom	63,047,162	15,400,000	52,731,209	83.6 %	2.2 %
10	France	65,630,692	8,500,000	52,228,905	79.6 %	2.2 %
11	Nigeria	170,123,740	200,000	48,366,179	28.4 %	2.0 %
12	Mexico	114,975,406	2,712,400	42,000,000	36.5 %	1.7 %
13	Iran	78,868,711	250,000	42,000,000	53.3 %	1.7 %
14	Korea	48,860,500	19,040,000	40,329,660	82.5 %	1.7 %
15	Turkey	79,749,461	2,000,000	36,455,000	45.7 %	1.5 %
16	Italy	61,261,254	13,200,000	35,800,000	58.4 %	1.5 %
17	Philippines	103,775,002	2,000,000	33,600,000	32.4 %	1.4 %
18	Spain	47,042,984	5,387,800	31,606,233	67.2 %	1.3 %
19	Vietnam	91,519,289	200,000	31,034,900	33.9 %	1.3 %
20	Egypt	83,688,164	450,000	29,809,724	35.6 %	1.2 %
TOP 20 Countries		4,664,486,873	273,374,200	1,776,355,028	38.1 %	73.8 %
Rest of the World		2,353,360,049	87,611,292	629,163,348	26.7 %	26.2 %
Total World Users		7,017,846,922	360,985,492	2,405,518,376	34.3 %	100.0 %

Fonte: Internet World Stats. http://www.internetworldstats.com/top20.htm.

No Brasil, o número de usuários ultrapassou os 88 milhões de usuários no ano de 2012 (Internet World Stats, 2013). Porém esse número é pequeno em relação a países tecnologicamente mais desenvolvidos e com população menor, como o Japão, por exemplo, país onde a Internet é amplamente utilizada.

De acordo com Garber (2007), a história mudou em quatro de outubro de 1957, quando a extinta União Soviética lançou com sucesso o primeiro satélite Sputnik I. Esse lançamento marcou o início de novos desenvolvimentos políticos, militares, tecnológicos e científicos.

Tudo começou em 1952 quando o Conselho Internacional de Uniões Científicas dos EUA decidiu em 01 de julho de 1957 criar uma comissão que, datou para 31 de dezembro de 1958 o lançamento de um satélite, pois este era o Ano Geofísico Internacional (AGI), período que apresenta ciclos de atividade solar em ativo e isto significa melhores condições para o lançamento (Garber, 2007) . Em outubro de 1954, o Conselho adotou uma resolução apelando para os satélites artificiais serem lançados durante o AGI.

Em julho de 1955, a Casa Branca anunciou planos para lançar um satélite em órbita da Terra. No mês de setembro do mesmo ano, a proposta da *Naval Research Laboratory's Vanguard* foi escolhida para representar os EUA durante o AGI.

Segundo Garber (2007) o lançamento do Sputnik mudou tudo. Como uma realização técnica, o Sputnik chamou a atenção do mundo e do público americano desprevenido. Seu tamanho era mais impressionante, além disso, o público temia que os soviéticos conseguissem lançar um satélite, pois assim eles também teriam capacidade de lançar mísseis balísticos capazes de transportar armas nucleares da Europa para os EUA. Para contrapor os avanços da URSS, o presidente dos EUA criou a *Advanced Research Project Agency (ARPA)* em outubro do mesmo ano.

A ARPA foi criada com um único objetivo principal, o desenvolvimento de programas relacionados a satélites e ao espaço. Além disso, para os Estados Unidos era essencial criar um método que garantisse a continuidade de operação das comunicações do governo, no caso de um ataque militar. O protótipo foi inaugurado em 1969, com a conexão entre quatro localidades: Universidades da Califórnia de Los Angeles, Santa Barbara, Universidade de Utah e Instituto de Pesquisa de Stanford, passando a ser conhecida como ARPANET.

Durante a evolução da ARPANET, foi estabelecida uma linguagem para que os computadores pudessem fazer a comunicação uns com os outros, denominada protocolo de comunicação, *Transmission Control Protocol / Internet Protocol* (TCP/IP), ainda utilizado nos dias de hoje, uma vez que a rede da ARPANET se tornava mais complexa, diversos protocolos além do TCP/IP foram criados.

A Internet chegou ao Brasil somente em 1988 (COSTA, 2006), por iniciativa do Laboratório Nacional de Computação Científica (LNCC) e da Fundação de Amparo à Pesquisa de São Paulo (FAPESP). “Dois anos depois em 1991, a FAPESP ficou encarregada da administração e distribuição dos endereços de IP do domínio.br”. Em maio de 1995, o Ministério das Comunicações e o Ministério da Ciência e Tecnologia decidiram que para tornar efetiva a participação da sociedade nas decisões envolvendo a implantação, administração e uso da Internet seria necessário a criação de um órgão gestor. Assim, criou-se um Comitê Gestor da Internet (CGI.br), que contaria com a participação dos Ministérios acima citados, de entidades operadoras e gestoras de espinhas dorsais de rede, de representantes de provedores de acesso ou de informações, de representantes de usuários e da comunidade acadêmica.

2.2 TCP – Transmission Control Protocol

O TCP é o protocolo responsável pela entrega dos dados transmitidos a um endereço IP. O endereço lógico na Internet ou IP deve ser único, representado por um conjunto de 32 bits. Tecnicamente, o atual IP é denominado IP versão 4, totalizando como comentado acima uma quantidade de 4.294.967.296. Porém essa quantidade de IP já se esgotou, em 01 de fevereiro de 2011. O órgão que supervisiona os endereços IP, *Internet Assigned Numbers Authority (IANA)* vendeu os dois últimos lotes de IP versão 4 de acordo com o site mybroadband.co.za.

A solução para o problema com a falta de IP versão 4 foi a criação do IP versão 6. Este novo protocolo é administrado por um conselho universitário dos Estados Unidos, o *University Corporation for Advanced Internet Development* (UCAID). Devido a forma como foi idealizada a versão 6 do protocolo, ela pode fornecer 340.282.366.920.938.000.000.000.000.000.000.000.000 de endereços IP únicos, solução para a falta de IP versão 4 de acordo com Morais (2009).

Com quantidades enormes de endereços de IP únicos geradas pelo protocolo IP versão 6 no inicio de sua implementação, a administração destes endereços pelos humanos se tornou impossível. Foi então que uma combinação foi proposta em 1983 por Paul Mockapertris: a tradução dos endereços do I*nternet protocol* para nomes, rotulados *domain name* (registro de domínio).

2.3 DNS - Domain Name System

O DNS segundo Costa (2007) foi criado devido a uma grande rede de comunicação que fomentou o surgimento da Internet. Com o crescimento da Internet veio à necessidade de mudar os esquemas primitivos de operação da rede, sendo o DNS um dos principais agentes modificadores destas operações na rede.

Em uma rede de comutação por pacotes (TANEMBAUM, 2003), endereços são utilizados para indicar o destino e a origem de um determinado pacote. Para os computadores é simples armazenar endereço de milhares de computadores, porém para os seres humanos esta tarefa não é nada simples. Uma solução inicial foi a criação de uma tabela que contivesse um mapeamento entre nome de computador e seu endereço. Esta tabela presente em todo computador era comumente chamada de host.txt.

O crescimento do número de computadores ligados à Internet aumentou bastante o tamanho desta tabela, o que impossibilitou sua gerencia. A alternativa adotada foi criar um sistema de tradução de nomes, esse sistema de tradução de nomes é conhecido como DNS.

No sistema DNS, o protocolo trabalha com nomes de domínios em vez de endereços IP (TANEMBAUM, 2003). Exemplos de nomes de domínios são: Yahoo.com, Google.com, domínio.com.br, entre outros. Como as comunicações na Internet utilizam endereços IP, os nomes de domínios são traduzidos em endereço IP (TANEMBAUM, 2003).

O serviço DNS é implementado como uma grande base de dados distribuída que tem a administração delegada a várias empresas e organizações de qualquer porte. A informação básica do serviço DNS é o domínio. Os domínios são representações textuais que fornecem informações sobre determinados hosts. Os domínios na Internet possuem uma hierarquia na forma de uma árvore invertida.

Um nome de domínio é sempre escrito seguindo um ponto mais especifico até um ponto menos especifico, de baixo para cima da árvore, além disso os nomes são separados por ponto final. Cada nó da árvore de domínios deve ser formado por qualquer combinação de letras, dígitos ou hífen, sendo que esse último não pode aparecer no começo ou no final do nome.

Para implementar o serviço DNS é necessário entender o paradigma cliente-servidor. O cliente quando realiza uma consulta de um IP de um determinado domínio, é chamado de cliente-DNS. O servidor que responde a consulta DNS é chamado simplesmente de servidor. Um servidor DNS contém informações de parte da árvore de domínios.

Uma consulta a um servidor DNS pode ser um pedido de tradução de um domínio em um endereço IP (TANEMBAUM, 2003), um pedido de tradução de um endereço IP em um domínio, ou ainda uma consulta de informação qualquer. As informações são armazenadas nos servidores DNS para posteriores consultas mais rápidas.

Os servidores DNS podem ser classificados em dois tipos principais: primários ou mestre e secundário ou escravo (TANEMBAUM, 2003). O servidor primário obtém os dados acerca das zonas sobre os quais ele tem autoridade. O servidor secundário obtém os dados de suas zonas de autoridade a partir de outros servidores que possuem autoridade sobre essas zonas. Outros tipos de servidores DNS são os de *cache* (apenas respondem com informações previamente consultadas), os *stub* (servidores que contém informações sobre os servidores com autoridade sobre determinados domínios) e os *forwarders* (utilizados para encaminhar consultas a outros servidores).

2.4 HTTP – Hyper Text Transfer Protocol

Na atual Internet o protocolo *HyperText Transfer Protocol* (HTTP) é a estrutura arquitetônica que permite o acesso aos documentos vinculados e espalhados em milhares de máquinas conectadas à grande rede (TANEMBAUM, 2003).

Segundo Tanembaum (2003), o protocolo de transferência mais utilizado em toda a *World Wide Web* (www) é o HTTP. Este protocolo especifica as mensagens que os clientes podem enviar aos servidores e que respostas eles receberão. Cada interação consiste em uma solicitação *American Standard Code for Information Interchange* (ASCII), seguida por uma resposta *Request for Comments* 822 (RFC 822), que é um documento que descreve os padrões de cada protocolo da Internet, semelhante ao *Multipurpose Internet Mail Extensions* (MIME). Os clientes e todos os servidores devem obedecer a esse protocolo, pois, ele é definido na RFC 2616.

De maneira geral, um navegador pode entrar em contato com um servidor estabelecendo uma conexão TCP para a porta 80 da máquina servidora, embora esse procedimento não seja exigido formalmente (TANEMBAUM, 2003). A vantagem de se usar o TCP é que nem os navegadores nem os servidores têm de se preocupar com mensagens perdidas, mensagens duplicadas, mensagens longas ou confirmações. Todos esses assuntos são tratados pela implementação do TCP. No HTTP 1.0 uma única solicitação era enviada e uma única resposta era devolvida. Então, a conexão TCP era encerrada. Num mundo no qual as páginas da *Web* típicas eram inteiramente em texto HTML, esse método era adequado.

Após alguns anos, a página da *Web* média passa a conter grandes números de ícones, imagens e outros atrativos visuais, e assim, o estabelecimento de uma conexão TCP para transportar um único ícone se tornou um modo de operação muito dispendioso.

Este problema levou ao lançamento do HTTP 1.1, que permite conexões persistentes, onde é possível estabelecer uma conexão TCP, enviar uma solicitação e obter uma resposta, e depois enviar solicitações adicionais e receber respostas adicionais. Amortizando o custo da instalação e da liberação do TCP por várias solicitações, o overhead relativo devido ao TCP é muito menor por solicitação (TANEMBAUM, 2003).

O protocolo HTTP foi projetado para utilização na *Web*, de usos mais gerais que o necessário, visando futuras aplicações orientadas a objetos. Um exemplo de sua utilização seria a comunicação de forma direta entre uma pessoa em um terminal (diferente de um navegador) e servidores da *Web*, com uma conexão TCP para porta 80 do servidor. Segundo Tanembaum (2003) com a seqüência abaixo de comandos, é possível uma comunicação:

```
telnet www.ietf.org 80 >log
GET /rfc.html HTTP/1.1
Host: www.ietf.org
close
```

> "Essa seqüência de comandos inicia uma conexão telnet (isto é, TCP) para a porta 80 no servidor da Web da IETF, www.ietf.org. O resultado da sessão é redirecionado para o arquivo log, a fim de ser inspecionado mais tarde. Em seguida, vem o comando GET que identifica o arquivo e o protocolo. A próxima linha é o cabeçalho Host obrigatório. A linha em branco também é necessária. Ela indica ao servidor que não existem mais cabeçalhos de solicitação. O comando close instrui o programa telnet a interromper a conexão."(TANEMBAUM, 2003)".

2.5 O protocolo SSL – Secure Sockets Layer

O *Secure Sockets Layer (*SSL*)* é definido por garantir segurança entre as conexões, segundo (TANEMBAUM, 2003). Quando a *Web* chegou ao público, foi usada apenas para distribuir páginas estáticas, mas após algum tempo, algumas empresas tiveram a idéia de usá-la para transações financeiras, como a compra de mercadorias por cartões de crédito e transações bancárias on-line. Essas aplicações criaram um aumento por conexões seguras. Em 1995, a Netscape Communications Corp, que na época dominava o mercado de fabricantes de navegadores, respondeu introduzindo um pacote de segurança chamado SSL para atender a essa demanda. Esse software e seu protocolo agora também são amplamente utilizados pelo *Internet Explorer.*

3 PRINCIPAIS ATAQUES E DEFESAS SOBRE O SERVIÇO DE *INTERNET BANKING* NO BRASIL

As principais fraudes causadas pelos ataques a serviços ou instituições financeiras existem desde que os serviços foram criados e implementados. Fraude é um termo que precede o surgimento da Internet, porém agora novas modalidades estão sendo utilizadas pelos criminosos, principalmente as que envolvem alta tecnologia. Iremos tratar o termo fraude neste capítulo como sendo um ato intencional de um fato que levará a obtenção de lucro ilícito, existindo a necessidade de três elementos principais para sua consumação: o fraudador, a vítima e o canal *Internet Banking* (LAU, 2004).

A maioria dos ataques cibernéticos registrados no Brasil (CERT, 2006), mais de 40% destes estão associados à tentativa de fraude sobre o ambiente da Internet sendo neste percentual sobre sites de comércio eletrônico, serviços de *Internet Banking*, cartas nigerianas entre outras tentativas. Os valores dos prejuízos causados não são muito divulgados, mas alguns dados de perdas por fraudes que envolviam *Internet Banking* em 2005 superaram os 300 milhões de reais (B2B Magazine, 2006), o que deve aumentar cada vez mais, devido aos avanços na tecnologia e ao crescimento da utilização de serviços bancários *online* (LAU, 2004).

Os tipos de ataques sobre o serviço de *Internet Banking* que serão abordados nesta monografia serão os que utilizam roubo de senha e os que utilizam falhas de segurança em servidores DNS. Nos capítulos abaixo serão detalhados estes ataques e os principais métodos de contenção.

4 ATAQUES UTILIZANDO ROUBO DE SENHAS

Os ataques que utilizam roubo de senha consistem basicamente em utilizar os logins e as senhas de contas roubadas para fazer transferência de valores para contas de "laranjas" (pessoas que ganham uma

parcela do dinheiro roubado em troca de fornecer contas bancárias para o crime) ou mesmo o pagamento de boletos pela Internet.

Segundo o Ministério Público Federal (MPF, 2007), as quadrilhas são estruturadas em uma divisão de funções que propiciam um efetivo crescimento exponencial das organizações criminosas que cometem este tipo de crime. As quadrilhas são divididas em indivíduos que irão executar sete funções básicas segundo a acessória do MPF em Minas Gerais (2008):

1) *Hacker* programador: indivíduo com capacidade técnica para desenvolver ou e/ou atualizar programa capaz de capturar dados sigilosos de terceiros através da Internet;

2) *Hacker*: indivíduo com certa capacidade técnica em informática, capaz de operar programas de computador destinados a capturar informações sigilosas como senhas, dados pessoais e dados bancários;

3) Biscoiteiro: indivíduo responsável por efetivar as transferências fraudulentas a partir dos dados fornecidos pelo *spyware* (programa espião que faz o furto da senha), gerenciando todo o negócio, inclusive a atuação dos carteiros e boleteiros. É responsável também pela distribuição do lucro;

4) Carteiro: indivíduo responsável por reunir cartões magnéticos e senhas de laranjas, pelos saques nos caixas eletrônicos e por acompanharem os laranjas, quando estes vão efetivar diretamente o saque na boca do caixa;

5) Boleteiro: indivíduo com função similar a do carteiro, responsável por reunir contas diversas e boletos a serem pagos pelo biscoiteiro;

6) Laranjas: pessoas que forneciam os dados e senhas de suas contas bancárias para serem utilizadas como destinatárias da fraude, recebendo entre 20% e 30% do valor sacado;

7) Beneficiários: indivíduo que tem suas contas pagas pelo biscoiteiro com o uso de recursos provenientes dos furtos. Para isso, ele devolve à quadrilha valor menor do que aquele devido no respectivo boleto.

A dificuldade no crime de roubo de senhas está na forma de como conseguir as senhas. Para isso os criminosos utilizam normalmente dois métodos: o uso de programas *sniffers* ou técnicas de engenharia social para tentar conseguir a senha diretamente com a vítima. Abaixo o detalhamento de como estes métodos funciona.

4.1 Sniffers

Os *sniffers* ou farejadores são os programas mais usados para conseguir senhas em uma rede. Eles normalmente ficam na memória dos computadores servidores ou pessoais analisando todo o tráfego da interface de uma rede. Qualquer informação (dado) que passa pela entrada ou saída da interface de rede é capturada, seja informação originada de um servidor FTP, ou de uma página de *chat* ou mesmo *e-mail* digitado. Os programas *sniffers* capturam os pacotes de dados recebidos e os transformam em texto puro para serem lidos. Estes programas são mais usados em sistemas Unix, mas ultimamente todos os outros sistemas operacionais como Microsoft Windows também possuem poderosos *sniffers* (FREITAS, 2007).

4.2 Filtrando os pacotes na rede

Para filtrar as informações, o *sniffer* é instalado em servidores centrais de uma rede para capturar os pacotes. Se este computador central pertencer a um provedor, por exemplo, todos os seus usuários que realizam o processo de autenticação neste computador terão seus pacotes capturados. Para instalar o *sniffer* a primeira coisa necessária é conseguir invadir o servidor e depois colocar o *sniffer*. O *sniffer* irá monitorar absolutamente todos os pacotes na rede, às vezes até informações pessoais dos usuários, como endereço e telefone. Devido a grande quantidade de pacotes em uma rede, o *sniffer* pode ser configurado para obter somente o essencial e importante: as senhas (FREITAS, 2007).

4.3 Capturando senhas

O interesse dos criminosos cibernéticos contra serviços de *Internet Banking* é capturar *logins* e senhas. Existem opções em alguns *sniffers* que possibilitam filtrar os tipos de pacotes recebidos. Após configurar o *sniffer*, o programa começa a enviar os pacotes capturados, e somente depois deste procedimento é possível filtrar o conteúdo dos pacotes para obtenção de *logins* e senhas, por exemplo, (FREITAS, 2007).

4.4 Sniffers em programas maliciosos

Alguns programas como o *Back Orifice* (BO) possuem a função de *sniffers* para serem instaladas como *plug-ins* (partes extras que podem ser anexadas ao programa). O *Buttsniffer* é um destes *plug-ins*, é considerado um dos melhores *plug-ins* para o BO, pois ele monitora absolutamente tudo em um sistema operacional Microsoft Windows. Além disso, ele possui um arquivo executável à parte, podendo funcionar

sem depender do *Back Orifice*. Alguns programas maliciosos possuem a função de *sniffer*, como por exemplo, o programa k2ps, ele monitora e envia todo tipo de senha importante por *e-mail* (FREITAS, 2007).

4.5 Sniffers em roteadores

Alguns *sniffers* conseguem obter dados direto do roteador. Mesmo que seja instalada uma proteção eficaz no sistema operacional, como um anti-sniffers, não adiantaria de nada se o programa estiver pegando os dados diretamente roteados. As correções têm de ser feita atualizando-se o próprio roteador (FREITAS, 2007).

4.6 Anti-sniffers

Para contenção de ataques contra o serviço de *Internet Banking* que utilizam *sniffers* devem ser utilizados programas que detectam tentativas de ataque ao sistema. Estes programas ficam residentes na memória como um anti-trojans, aguardando o invasor tentar algo. Há vários tipos de anti-sniffers. A utilização de programas que removem arquivos ou programas maliciosos também é recomendada para conter ataques que visam roubo de senha utilizando *sniffers* (FREITAS, 2007).

5 ENGENHARIA SOCIAL

A engenharia social é uma tática usada pelos criminosos cibernéticos. É o que a lei chama de estelionato. É basicamente uma tentativa de enganar uma pessoa realizada por outra para se conseguir vantagens. Como exemplo, uma pessoa que liga para o provedor e pergunta informações sobre os servidores ou senhas de usuários. Alguns provedores pedem documentação para comprovar que quem esta ligando é o verdadeiro dono da conta, outros (que podem ter funcionários insatisfeitos) não perguntam as informações de quem esta ligando, chegando a passar até o número do cartão de crédito de algum usuário se lhe for pedido (ASSUNÇÃO, 2002).

A melhor forma de evitar este tipo de ataque é educando a população e divulgando aos usuários que este tipo de ataque existe e todos devem seguir as normas de segurança estipuladas pela empresa, provedor ou especialistas da área (FREITAS, 2007).

6 ATAQUES UTILIZANDO SERVIDORES DNS

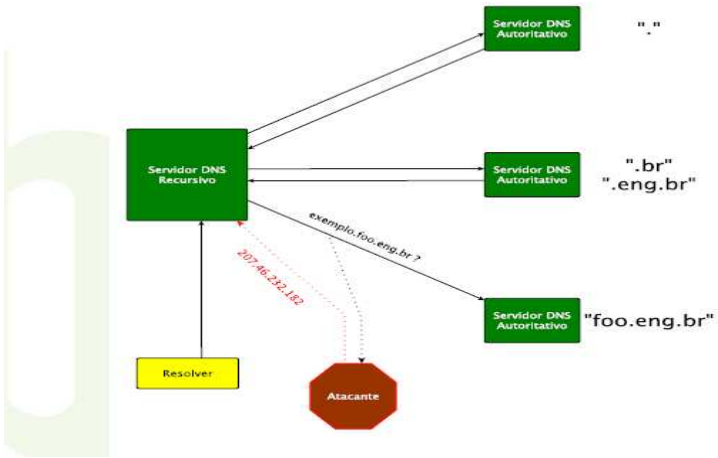
Existem tipos de ataques contra o serviço de *Internet Banking* que não utilizam o roubo de *login* e senha. No próximo capítulo iremos entender o funcionamento de um destes ataques, o *pharming,* (LAU, 2004).

7 ATAQUE UTILIZANDO *PHARMING*

O *pharming* é um conceito recente ao público mundial, porém ele foi um meio muito utilizado para fraude em serviço de *Internet Banking* no Brasil (LAU, 2010). O mecanismo utilizado por este ataque é realizar um redirecionamento da vítima para páginas falsas de instituições financeiras. O atacante utiliza falhas de segurança dos serviços de resolução de nomes na Internet, o DNS, que resultam em acesso errado do usuário às páginas das instituições financeiras, mesmo se o usuário digitar o endereço da página do banco na URL do *browser* este redirecionamento vai ser feito (LAU, 2004).

Este ataque normalmente é feito utilizando a poluição do cache do servidor DNS, o atacante normalmente descobre o IP do servidor DNS de um determinado local e encaminha pacotes que tentam responder mais rápido a resolução de nome que o DNS autoritativo. Observe a figura 3 para entender o funcionamento do ataque (JUSTO, 2010).

Figura 3. Poluição de cache em servidor DNS.



Fonte : Introdução a DNS & DNSSEC, JUSTO, 2010.

O atacante fornece uma informação errada sobre a resolução de um endereço e fornece essa informação ao DNS recursivo que iria entregar a informação falsa ao cliente, podendo ser um IP de um site de banco falso. No próximo capitulo iremos verificar medidas de contenção contra o *pharming.*

7.1 Medidas de contenção contra o Pharming

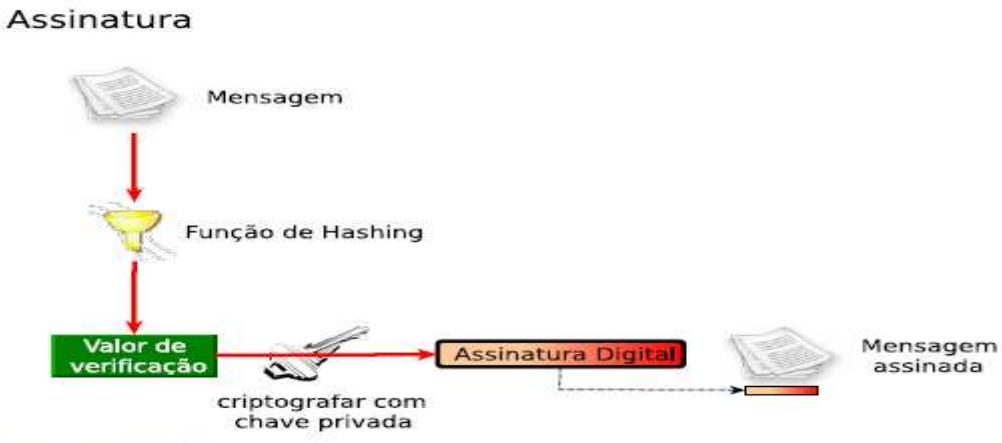
Para conter um ataque que utiliza técnicas de *pharming* pode ser utilizar um certificado digital ou configurar os servidores DNS com a ferramenta Dnssec (LAU, 2004). Nos próximos capítulos vamos entender o funcionamento das defesas para o ataque tipo *pharming*.

8 CERTIFICADO DIGITAL

O certificado digital é um documento eletrônico que possibilita comprovar a identidade de uma pessoa, uma empresa ou um site, para assegurar as transações online e a troca eletrônica de documentos, mensagens e dados, com presunção de validade jurídica.

O certificado digital é composto por uma chave privada que é uma das chaves utilizadas no processo de criptografia assimétrica e uma chave pública. Neste processo são utilizados pares de chaves públicos e privados. A chave pública é divulgada aos membros que realizam comunicação e é utilizada para a encriptação de dados (LAU, 2004). A chave privada é gerada e armazenada com o dispositivo do usuário responsável pela guarda do certificado. A chave privada consegue decriptar uma mensagem encriptada pela chave pública. As figuras 4 e 5 demonstram claramente o funcionamento de chaves simétricas (JUSTO 2010).

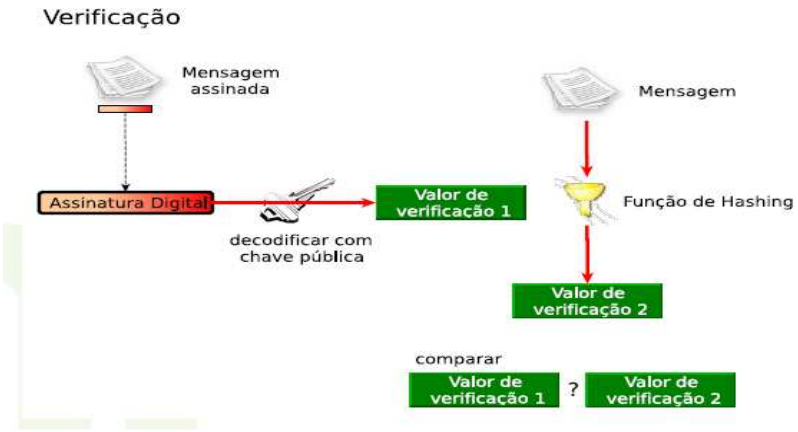
Figura 4: Chaves assimétricas assinatura.



Fonte: Introdução a DNS & DNSSEC, JUSTO, 2010.

A figura acima mostra o funcionamento da assinatura da mensagem, uma função *hash*, (um algoritmo que realiza cálculos sobre a mensagem e que gera um código), um código é criado e outro algoritmo de criptografia age sobre a mensagem, utilizando a chave pública. A mensagem assinada junto com o código de *hash* é enviada ao destino (LAU, 2004).

Figura 5: Chaves assimétricas verificação.



Fonte: Introdução a DNS & DNSSEC, JUSTO, 2010.

Já a figura 5 demonstra a verificação da mensagem enviada pela origem, a mensagem é decodificada, utilizando a chave privada, após a decodificação é aplicado sobre a mensagem decriptografada o algoritmo *hash*, o código resultante é comparado com o código que foi enviado junto com a mensagem pela origem. Se os valores dos códigos forem iguais a mensagem pode ser considerada autêntica (JUSTO, 2010).

A chave privada pode ser armazenada no sistema operacional ou em algum equipamento que permite a inserção de dados cifrados resultantes da decriptação, não permitindo extração ou leitura da chave privada (LAU, 2004).

No Brasil os certificados são classificados pelo Governo Federal nas classes A1, A2 e A3. A classe A1 guarda o certificado em sistema operacional e a A3 faz o armazenamento do certificado em dispositivos especializados, sensíveis à temperatura, atividades sísmicas e tentativas de violação. Os clientes que possuem serviços de *Internet Banking* recomenda-se o uso de certificação A2, que faz o armazenamento do certificado em *smart card,* um cartão plástico que possui um *chip* (LAU, 2004).

9 DNSSEC – Domain Name System Security Extensions

O *Domain Name System Security Extensions (*DNSSEC) é uma configuração realizada sobre o DNS que visa garantir a segurança dos servidores DNS. O DNSSEC provê segurança para a resolução de endereços uma vez que funciona como um caminho alternativo para a verificação de autenticidade. O DNSSEC não é uma nova ferramenta de resolução de nomes ela é apenas uma extensão do serviço DNS, o DNSSEC garante autenticidade da origem, ou seja, quem responde a resolução de nome é o DNS recursivo verdadeiro. Na figura 6 é possível observar o perímetro virtual em que o DNSSEC atua (JUSTO, 2010).

Figura 6. DNSSEC sobre o DNS recursivo.

Fonte: Introdução a DNS & DNSSEC, JUSTO, 2010.

O funcionamento do DNSSEC ocorre sobre a comunicação servidora DNS recursivo e os servidores DNS *master* e *slave*. O processo de segurança utiliza os conceitos já explicados acima de chave assimétrica e o algoritmo de *hash*. O DNS recursivo como pode ser comparado à origem do exemplo do capitulo anterior e o DNS *master* ou o *slave* ao destino. Desta forma os servidores garante autenticidade entre eles, no caso de uma tentativa de poluição de *cachê* o servidor recursivo irá recusar as informações do atacante (JUSTO, 2010).

10 PRINCIPAIS ALVOS DOS ATAQUES

Segundo *o site www.safernet.org.br*, que é considerado por muitos especialistas como uma entidade de referência nacional contra crimes e violações aos direitos humanos na Internet, em fevereiro deste ano, os casos que foram mais registrados sobre crimes na Internet são os envolvendo pornografia, homofobia, crimes contra a vida e crimes contra o serviço de *Internet Banking*. Com o aumento do número de usuários as informações pessoais ficam cada vez mais expostas e a privacidade cada vez menor.

Os serviços de advocacia e defesa para crimes citados acima são mais procurados por contas jurídicas, em sua maioria as vítimas são principalmente idosos e crianças segundo Lobosco (2006).

> "Os sujeitos mais suscetíveis a serem alvos de crimes virtuais são aqueles com menor familiaridade à maturidade para lidar com temas tecnológicos, dentre eles a navegação na Internet. Neste cenário, crianças e idosos, assim como em outros tipos de fraudes, tendem a serem as vítimas mais comuns".

Em decorrência do grande fluxo de informações da Internet, alguns serviços (*Orkut, Facebook* e etc.) não conseguem fiscalizar ativamente todo o conteúdo hospedado por seus usuários. Estes serviços apenas retiram conteúdos indevidos quando informados, seja via mecanismo próprio ou por ordem judicial.

> "Não há uma lei específica para crimes virtuais, mas isso não significa que estejamos desprotegidos. Os mecanismos legais são adaptáveis para o cenário virtual e, em sua grande maioria, funcionam sem maiores problemas" (LOBOSCO, 2006).

No Brasil, este cenário sem leis específicas e com jovens e idosos mais vulneráveis não deve mudar nos próximos anos se não ocorrerem grandes modificações na sociedade brasileira. Algumas medidas já estão sendo criada para alterar esta situação. O Brasil, por meio de um projeto desenvolvido pela Federação Brasileira dos Bancos (FEBRABAN), órgão que representa várias instituições financeiras - começou um processo para conscientização de seus usuários (LOBOSCO, 2006).

No início do ano 2006 aconteceu a primeira coletiva de imprensa tendo como objetivo a orientação sobre fraudes junto à população. Antes deste evento, nenhuma instituição financeira tinha feito um pronunciamento oficial sobre o assunto. Iniciativas com a da instituição FEBRABAN buscam transparência ao assunto e visa esclarecer os clientes (principalmente os bancários) dos perigos sobre os crimes e as medidas de segurança que eles devem tomar tornando-os menos suscetíveis aos crimes de fraude pela rede, Estas medidas buscam ao mesmo tempo garantir segurança e incentivar o uso do serviço de *Internet Banking* pelos usuários, o que é muito vantajoso para as instituições financeiras já que o *Internet Banking* resulta no menor custo transacional no processo de intermediação financeira dentre os serviços oferecidos pelos bancos (LAU, 2004).

11 CONCLUSÃO

Ao término deste trabalho, reafirma-se os objetivos traçados, que foram de analisar a história e a evolução do serviço de *Internet Banking* no Brasil bem como a análise de alguns ataques praticados contra o serviço e os métodos de contrapor estes ataques. As idéias pesquisadas e discutidas permitem formular, algumas conclusões.

Verificou-se que a *Internet* é essencial nos dias de hoje para impulsionar o desenvolvimento e a economia de um país. O setor bancário de um país tem influência direta para que estas modificações ocorram. Foi discutido também que para o setor bancário o aumento na utilização dos serviços pela I*nternet* é vantajoso, pois diminui custos, uma vez que sua utilização propicia um menor número de pessoas para as operações. Em decorrência deste fato alguns bancos no Brasil foram pioneiros na utilização do serviço de *Internet Banking*.

Constatou-se também que o crescimento contínuo da I*nternet* no Brasil está provocando um aumento no uso do serviço de *Internet Banking*. Este aumento no uso de tecnologias deve provocar um ambiente mais propício para ações de criminosos pela Internet. Para entender melhor como aumentar a segurança na Internet, foi necessário analisar algumas ferramentas e programas que os criminosos utilizam para cometer os crimes. Durante as pesquisas ficou claro que os criminosos cibernéticos estão cada vez mais sofisticados.

As quadrilhas estão cada vez melhor estruturadas, com divisões de tarefas, incluindo ate mesmo função de gerência.

Nos ataques estudados normalmente são programas que analisam tráfego de redes ou mesmo redirecionam informações bancárias. Algumas técnicas de engenharia social também podem ser utilizadas para as ações criminosas. Algumas medidas para conter estes ataques já estão sendo tomadas por entidades responsáveis pela I*nterne*t no Brasil e no mundo e também as entidades que representam o setor bancário, como a FEBRABAN. Porém ficou claro nas pesquisas deste trabalho que o usuário é o maior prejudicado nos ataques e deve partir dele a conscientização para não cair nas armadilhas criadas pelos criminosos cibernéticos. Confirma-se também que os principais alvos dos ataques e crimes cometidos na Internet e contra o serviço de *Internet Banking* são os mais jovens e os idosos.

É possível concluir então que a utilização do serviço de *Internet Banking* no Brasil esta aumentando e os ataques ao serviço estão cada vez mais comuns. O governo e sociedade brasileira pouco tem feito para conscientizar a população sobre os riscos da utilização deste serviço. Espera-se que em um futuro próximo as informações sobre os ataques e as principais formas de proteção sejam mais divulgadas e que ocorra um amadurecimento na utilização dos serviços e ferramentas disponibilizadas na I*nternet*, entre elas o *Internet Banking.*

REFERÊNCIAS

ASSUNÇÃO, Marcos Flávio Araújo. **Guia do hacker brasileiro**. São Paulo, 2002.

CARMONA, Tadeu, **Universo hacker.** 2.ed. São Paulo: Digerati, 2006.

COMER, Douglas E. **Internetworking with TCP/IP**. 4.ed. New Jersey: Printice Hall, 2000.

COSTA, Daniel G. **DNS***:* um guia para administradores de redes*.* Rio de Janeiro: Brasport, 2006.

D'ANDRÉA, Edgar R. P. et al. **Segurança em banco eletrônico**. Coordenador: D'ANDRÉA, Edgar R. P. São Paulo: Pricewaterhouse & Coopers, 2000.

DINIZ, Eduardo H. Cinco décadas de automação. **GV–Executivo**. Editorial Era Digital. Edição especial 50 anos. FGV–EAESP, São Paulo, v. 3, n. 3, p. 58, ago./out. 2004.

DINIZ, Eduardo H.; PORTO, Roseli; ADACHI, Tomi. ***Internet Banking* sob a ótica da funcionalidade, confiabilidade e usabilidade.** In: Conselho Latino Americano de Escolas de Administração, 38, 2003, Peru (Lima). ANAIS DO CLADEA, 2003.

FILIPPETTI, Marco Aurélio. **CCNA 4.1:** guia completo de estudo. Florianópolis: Visual Books, 2008.

GOMES, Alessandra Aparecida Calvoso. Operações bancárias via Internet (*Internet Banking*) no Brasil e suas repercussões jurídicas. In **Revista dos Tribunais**, vol. 816, outubro de 2003.

NEMETH, Evi.; SNYDER,Garth.;HEIN,Trent R. ***Manual completo do DNS***. São Paulo: Pearson Makron Books, 2004.

TANENBAUM, A. C. **Redes de computadores**. 4.ed. São Paulo: Campus, 2003.

TAPSCOTT, Don**. Economia digital**. São Paulo: Makron Books, 1997.

THOMPSON, Marco Aurélio. **Invasão. BR**, vol. 1: invasões comentadas passo-a-passo e em vídeo aulas. 2.ed. Salvador; ABSI - Associação Brasileira de Segurança na Internet, 2005.

ZANIOLO, Pedro Augusto. **Crimes modernos**: o impacto da tecnologia no direito. Curitiba: Juruá, 2007.

Referências eletrônicas

B2B Magazine. <http://www.b2bmagazine.com.br/seguranca/dia-da-internet-segura>. Acesso em 15 de maio de 2011.

Central Intelligence Agency. <https://www.cia.gov/library/publications/the-worldfactbook/rankorder/2153rank.html>. Acesso em 4 Agosto de 2008.

CENTRO DE ESTUDOS SOBRE AS TECNOLOGIAS DA INFORMAÇÃO E DA COMUNICAÇÃO. TIC domicílios e usuários 2009. Disponível em <http://www.cetic.br/usuarios/tic/2007/index.htm> Acesso em 22 Fevereiro de 2011.

CERT.br - Incidentes Reportados ao CERT.br -- Outubro a Dezembro de 2005. Disponível em: < http://www.cert.br/stats/incidentes/2005-jul-sep/tipos-ataque.html> Acesso em: 05 fev. 2006.

CGI.BR.<http://www.cgi.br/publicacoes/revista/edicao03/txt.htm>. Acesso em 03 de Abril de 2011.

Data Interchange Software Solutions. <http://www.di2s.com/edi.htm#>. Acesso em 03 de Abril de 2011.

Ebit empresa.<www.ebitempresa.com.br/ index_ebitinforma.htm>, acesso em 04 de Março de 2011.

FREITAS, Josué Paulo José, Como evitar ataques de engenharia social. <http://www.linuxsecurity.com.br/sections.php?op=viewarticle&artid=21>. Acesso em 20 de Maio de 2011.

IBGE.<ftp://ftp.ibge.gov.br/Contagem_da_Populacao_2007/>.Acesso em 14 de Março de 2008.

LAU, Marcelo. Técnicas utilizadas para efetivação e contenção das fraudes sobre Internet Banking no Brasil e no mundo <http://www.datasecur.com.br/academico/Tecnicas_Utilizadas_para_Efetivacao_e_Contencao_das_fraudes.pdf>.Acesso em 20 de Maio de 2010.

MOREIRAS, Antonio. Entenda o esgotamento do IPv4. <http://www.ipv6.br/IPV6/ArtigoEsgotamentoIPv4>. Acesso em 9 de Abril de 2011.

Mybroadband.<http://mybroadband.co.za/news/internet/18157-IPv4-addresses-now-finished-and-klaar.html>.Acesso em 9 de Abril de 2011.

O Globo. http://oglobo.globo.com/economia/mat/2007/06/14/296169156.asp>, acesso em 03 de Março de 2011.

O Globo. http://oglobo.globo.com/tecnologia/mat/2010/02/01/brasil-um-dos-paises-mais-vulneraveis-ataques-ciberneticos-diz-pesquisa-915752843.asp acesso em 10 de Março de 2011.

Procuradoria Geral da República.<http://noticias.pgr.mpf.gov.br/noticias/noticias-do-site/copy_of_criminal/mpf-mg-denuncia-51-pessoas-que-praticavam-furtos-pela-internet>. Acesso em 10 de Maio de 2001.

RAMOS, Anatália Saraiva Martins. Serviços bancários pela internet: um estudo de caso integrando a visão de competidores e clientes. <http://www.scielo.br/scielo.php?pid=S141565552000000300008&script=sci_arttext>.Acesso em 02 de Abril de 2011.

RIBEIRO, Mário César. TRF1. RECURSO CRIMINAL 2007.38.00.03 6480-7/MG Relator: Desembargador Federal Mário César Ribeiro Julgamento: 25/08/09.<Disponível http://www.centraljuridica.com/jurisprudencia/t/563/crime_na_internet.html>. Acesso em 22 Fevereiro de 2011.

TELECO Inteligência em Telecomunicações.<http://www.teleco.com.br/tutoriais/ tutorial mplseb1/pagina_2.asp>. Acesso em: 15 de maio de 2011.

Rafael Vaz Gallao

Possui graduação em ANALISE DE SISTEMAS COM ENFASE EM SEGURANÇA DA INF pela FATEC AMERICANA(2011)
Contato: leafarvaz@hotmail.com
Fonte: CNPQ – Currículo Lattes

Alberto Martins Junior

Possui graduação em Tecnologia em Processamento de Dados pela Universidade Metodista de Piracicaba (1992) , especialização em Análise de Sistemas pela Universidade Metodista de Piracicaba (1993) , especialização em Formação Pedagógica Docentes Educ Prof. Ensino Méd pela Universidade Metodista de Piracicaba (2000) e mestrado em Administração de Empresa pela Universidade Metodista de Piracicaba (2004) . Atualmente é Analista de Suporte da Universidade Metodista de Piracicaba, Professor da Escola de Engenharia de Piracicaba, Coordenador Curso Superior de Administração da Escola de Engenharia de Piracicaba e Professor da Faculdade de Tecnologia Americana. Tem experiência na área de Administração, com ênfase em Sistemas de Informação. Atuando principalmente nos seguintes temas: Sistema de Informação, Tecnologia da Informação, Sistema de Informação Gerencial.
Contato: amartins@unimep.br
Fonte: CNPQ – Currículo Lattes