CENTRO PAULA SOUZA
GOVERNO DO ESTADO DE SÃO PAULO

Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Análise de Sistemas e Tecnologia da Informação com ênfase em segurança de redes

SEGURANÇA DO INTERNET BANKING NO BRASIL

Rafael Vaz Gallão

Americana, SP

2011

CENTRO PAULA SOUZA
GOVERNO DO ESTADO DE SÃO PAULO

Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Análise de Sistemas e Tecnologia da Informação com ênfase em segurança de redes

SEGURANÇA DO INTERNET BANKING NO BRASIL

Rafael Vaz Gallão

Trabalho monografia por Rafael Vaz Gallão como exigência do curso de graduação em análise de sistemas e tecnologia da informação com ênfase em segurança de redes da Faculdade de tecnologia de Americana sob a orientação do professor Alberto Martins Junior.

Americana, SP
2011

BANCA EXAMINADORA

Prof. Alberto Martins Junior

_____

Prof. Ivan Menerval da Silva

_____

Prof. Rogério Nunes de Freitas

_____

AGRADECIMENTOS

Ao mestre professor Alberto Martins Junior, pelo auxílio e compreensão, fatores que influenciaram de forma significativa neste trabalho.

A professora Maria Cristina Aranda Batocchio pelo apoio e orientação na metodologia apresentada.

A universidade Fatec Americana por todas as oportunidades que surgiram e que irão surgir.

A minha família, em especial para minha mãe que sempre foi meu suporte para continuar os estudos e terminar a faculdade.

A minha esposa que me auxiliou nas correções e idéias para a conclusão deste trabalho.

RESUMO

Este trabalho apresenta uma pesquisa realizada sobre a história e o funcionamento do serviço de *Internet Banking* no Brasil desde sua criação. O trabalho ainda 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 estas informações para desviar quantias de dinheiro de maneira criminosa. Outra forma de realizar roubo ou furto de senhas que será comentada neste trabalho é a utilização de engenharia social, que é basicamente o ato de enganar pessoas, usuários ou clientes para se conseguir vantagens, é o que a lei chama de estelionato. Outro método de ataque ao serviço de *Internet Banking* também comentado neste trabalho é o ataque sobre o servidor de nomes o DNS. Estes ataques normalmente são feitos por criminosos que tentam responder com informações erradas as solicitações de uma resolução de nome que um cliente faz a um servidor DNS. Um site de banco falso também é usado no ataque, no momento em que o usuário utiliza o site falso o criminoso comete o ataque, pois este site falso pode conter inúmeras armadilhas para o usuário. Além das abordagens sobre os ataques descritos acima, também serão comentadas as defesas para estes ataques e quem são os principais alvos destes ataques na internet.

Palavras chaves: 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 is the use of programs that analyze the data traffic on a network and selects the information regarding the login and passwords, so the criminals can get information, for example, the logins and passwords, and use this 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 also mentioned in this work is the attack on the DNS name server. These attacks are usually done by criminals who try to respond with incorrect information requests 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.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS DE ABREVIATURAS

AGI - Ano Geofísico Internacional

ARPA - *Advanced Research Projects Agency*

ARPANET - *Advanced Research Projects Agency Network*

ASCII - *American Standard Code for Information Interchange*

CERT. BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CGI - Comitê Gestor da Internet

DNS - *Domain name system*

DNSSEC - *Domain Name System SECurity extensions*

EDI - *Electronic Data Interchange*

EUA - Estados Unidos da América

FAPESP - Fundação de Amparo à Pesquisa de São Paulo

FTP - *File transfer protocol*

HTML - *HyperText Markup Language*

HTTP - *Hypertext Transfer Protocol*

IBGE - Instituto Brasileiro de Geografia e Estatística

IETF – *Internet Engineering Task Force*

IP - *Internet protocol*

ISO - *International Organization for Standardization*

NASA - *National Aeronautics and Space Administration*

OSI - *Open Systems Interconnection*

RFC - *Request for Comments*

SNMP - *Simple Network Management Protocol*

SSL - *Secure Sockets Layer*

URL - *Uniform Resource Locator*

URSS - União das Repúblicas Socialistas Soviéticas

WWW - *World Wide Web*

SUMÁRIO

1 INTRODUÇÃO

Este trabalho foca a evolução da segurança para utilização do *Internet Banking*. Foram analisados dados estatísticos sobre alguns tipos de ataques, além dos impactos causados pelos ataques no *Internet Banking* no Brasil e os principais alvos.

Os crimes cibernéticos praticados contra o serviço de *Internet Banking* no Brasil são para os especialistas os mais comuns, já que na maioria dos casos os ataques visam diretamente o crime de roubo como cita 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 do Brasil no Centro de estudos sobre as Tecnologias da Informação e da Comunicação – TIC (2009).

> "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."

Com o aumento dos acessos à Internet é provável que mais vulnerabilidades de segurança sejam identificadas e serviços como o *Internet Banking* sejam alvos cada vez mais alvo de ataques.

1.1 OBJETIVOS

Para possibilitar um melhor entendimento sobre o volume e os riscos dos crimes cibernéticos praticados contra o serviço de *Internet Banking*, este trabalho visou mostrar a evolução da segurança do serviço *Internet Banking* desde sua criação ate os dias de hoje, além disso foi apresentado técnicas utilizadas por criminosos para ataque e quais as defesas contra estes ataques sobre o serviço de *Internet Banking* no Brasil.

1.1.1 OBJETIVO GERAL

O objetivo geral deste trabalho é pesquisar e analisar dados estatísticos e científicos na área de tecnologia de informação e segurança, com o objetivo de pesquisar e dar indicativos sobre os ataques praticados no serviço de *Internet Banking* no Brasil.

1.1.2 OBJETIVOS ESPECÍFICOS

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, utilizando-se a seguinte programação:

a) Entender a evolução, utilização e a história do serviço de *Internet Banking* no Brasil, tendo como base as referências:

- Quem introduziu e quando o serviço surgiu no Brasil, identificando as primeiras instituições no Brasil a utilizar o serviço.
- Pesquisar e analisar dados estatísticos sobre a evolução da segurança no serviço.

b) Definir e analisar os principais ataques e defesas em relação ao serviço de *Internet Banking* no Brasil.

- Análises de crimes cibernéticos cometidos visando o roubo de senhas, como a utilização de *sniffers* que de acordo com o Thompson (2005) são programas que filtram dados na rede e capturam senhas. O autor argumenta que os *sniffers* atuais também podem ser instalados remotamente em um computador facilitando assim sua utilização pelos criminoso cibernéticos. Outra ferramenta utilizada pelos criminosos são as técnicas de engenharia social que é definida por Carmona (2006), como:

> "A engenharia social consiste em, através de subterfúgios – que enganem um usuário, grupo deles, ou mesmo um sistema – ser capaz de coletar informações sobre o funcionamento de um servidor, rede de computadores ou mesmo uma lista de senhas".

O autor também cita que a maioria dos criminosos que utilizam técnicas de engenharia social costuma agir bem longe do teclado e do mouse, eles apostam na sua capacidade de enganar através de telefones, conversas ou mesmo utilizando correio ou mensagens eletrônicas.

- Foi feito uma análise de crimes cibernéticos praticados contra servidores DNS que é definido por Tanembaum (2003) como**:**

> "A essência do DNS é a invenção de um esquema de atribuição de nomes hierárquico, baseado em domínios. Ele é principalmente usado para mapear nomes de host e destinos de mensagens de correio eletrônico em endereços IP, mas também pode ser usado para outros objetivos."

O autor também complementa que DNS é também um serviço para mapear um nome em um endereço IP. Assim uma tabela ou biblioteca de informações é consultada e o serviço DNS resolve, ou traduz um nome para um endereço IP. Estes ataques a servidores DNS em conjunto com web sites falsos, criam um tipo de ataque chamado *pharming*, que é definido como uma técnica que altera a tabela DNS de um servidor de resolução de nomes fazendo com que as requisições a determinada página sejam redirecionadas para web sites falsos (THOMPSON, 2005).

- Análise do público alvo mais suscetível aos ataques e sobre políticas de segurança em tecnologia da informação para conter os ataques ao serviço de *Internet Banking* no Brasil.

2 JUSTIFICATIVA DO ESTUDO

Cada vez mais é possível observar o aumento 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 aumentou 37% entre os anos de 2001 a 2006. Em decorrência deste aumento 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 aumento do consumo dos serviços bancários o aumento de fraudes e crimes aumentam também, principalmente os crimes cibernéticos uma vez que se observa um aumento da utilização da tecnologia em nosso país, 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 utilização 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.

3 ORGANIZAÇÃO DO TRABALHO

O método de procedimento deste trabalho foi o monográfico, sendo o método de pesquisa o bibliográfico. Para conclusão desta pesquisa segue-se o seguinte plano de desenvolvimento.

Além desse capítulo introdutório, o trabalho conta com um quarto capítulo que abordou informações sobre o serviço *Internet Banking*: o que é o serviço; quais seus principais objetivos; o perfil de usuários e instituições que o utilizam e como ele é usado, além disso, foi apresentando sucintamente o histórico do serviço *Internet Banking*.

No quinto capítulo foram apresentadas as definições e explicações sobre os termos técnicos utilizados no trabalho. Termos como: redes de computadores; internet; protocolos de redes e segurança. Numa aproximação maior do tema proposto o sexto capítulo mostra os principais ataques e suas defesas contra o serviço *Internet Banking*.

Para finalizar, o trabalho possui uma conclusão sobre as pesquisas apresentadas bem como uma possível dedução do futuro da segurança no serviço de *Internet Banking*.

4 INTERNET BANKING

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

Para Diniz (2003) os bancos tem se desenvolvido ao longo dos tempos, principalmente com 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. Na década de 90 surgiu o que Tapscoot (1997) chamou de "Economia Digital", definindo-a da seguinte forma:

> "Estamos no limiar de uma nova economia digital, onde os microprocessadores e as redes públicas que seguem o modelo da Internet possibilitam tipos fundamentalmente novos de estruturas institucionais e de relacionamentos. O que está acontecendo é isto: indivíduos eficientes, trabalhando em estruturas de equipe de alto desempenho; transformando-se em redes organizacionais e integradas, com clientes e servidores: que saem ao encontro de clientes, fornecedores, grupos de afinidade e até mesmo concorrentes; que se conectam a Net pública, alterando amaneira como produtos e serviços são criados, comercializados e distribuídos."

É possível visualizar essa evolução do sistema bancário brasileiro observando a linha temporal ilustrada na figura 1 abaixo (DINIZ, 2004.).

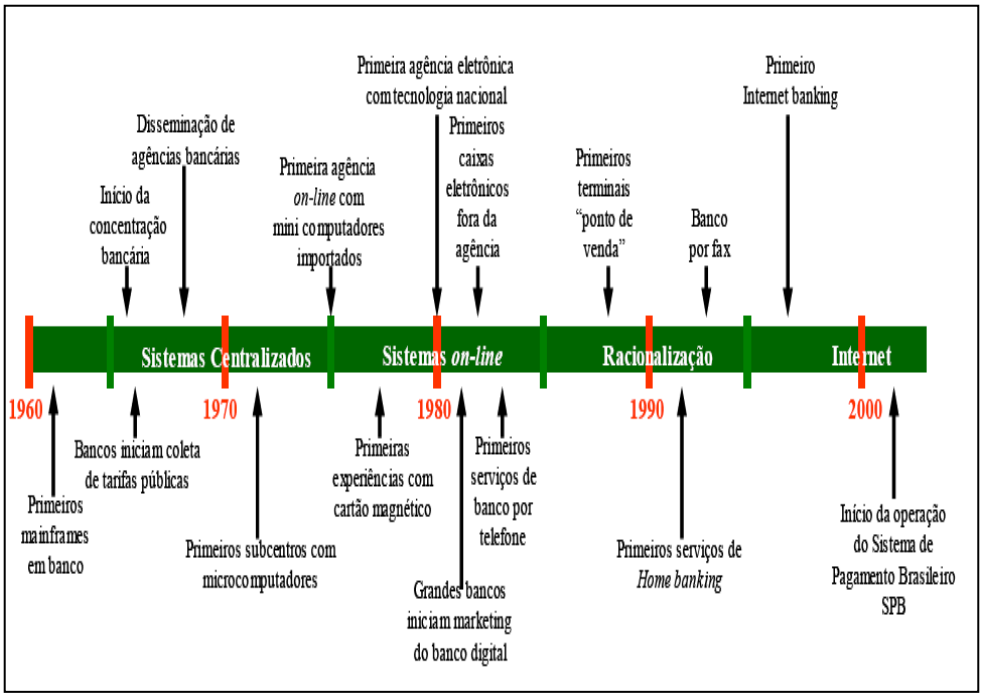

Figura 1: Fases da automação bancária no Brasil.
Fonte: (DINIZ, 2004).

Com o evento da economia digital (TAPSCOTT, 1997) foi possível à criação de um serviço chamado *Internet Banking*. O Brasil foi um dos países pioneiros na utilização deste 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 a utilização do serviço de *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 HTML (*Hyper Text Markup Language*) uma linguagem de computador muito utilizada para construir sites. Já o termo rede *dial-up* é um tipo de acesso a Internet no qual o cliente utiliza um modem e uma linha telefônica para o acesso. Segundo o site www.dip.co.uk o termo EDI (*Electronic Data Interchange*) 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 e-bit, 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 banco que possui mais clientes cadastrados para utilizar o serviço.

O aumento da compra de computadores e o aumento na utilização da Internet afetam diretamente o uso do *Internet Banking*, dados da pesquisa TCI (tecnologias da informação e da comunicação) 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: NIC.Br (2010).

Na tabela 1 fica nítido o aumento do uso da internet no Brasil. Pode-se observar que a população brasileira teve um crescimento em milhões de 12,7 % durante os anos de 2000 a 2009 e o crescimento da internet para este mesmo período foi de 642,8 %. Este crescimento foi bem expressivo e tende a aumentar ainda mais pois os dados de 2009 mostram que apenas um terço da população brasileira possui acesso à internet. A figura 2 reforça ainda mais esta tendência de crescimento.

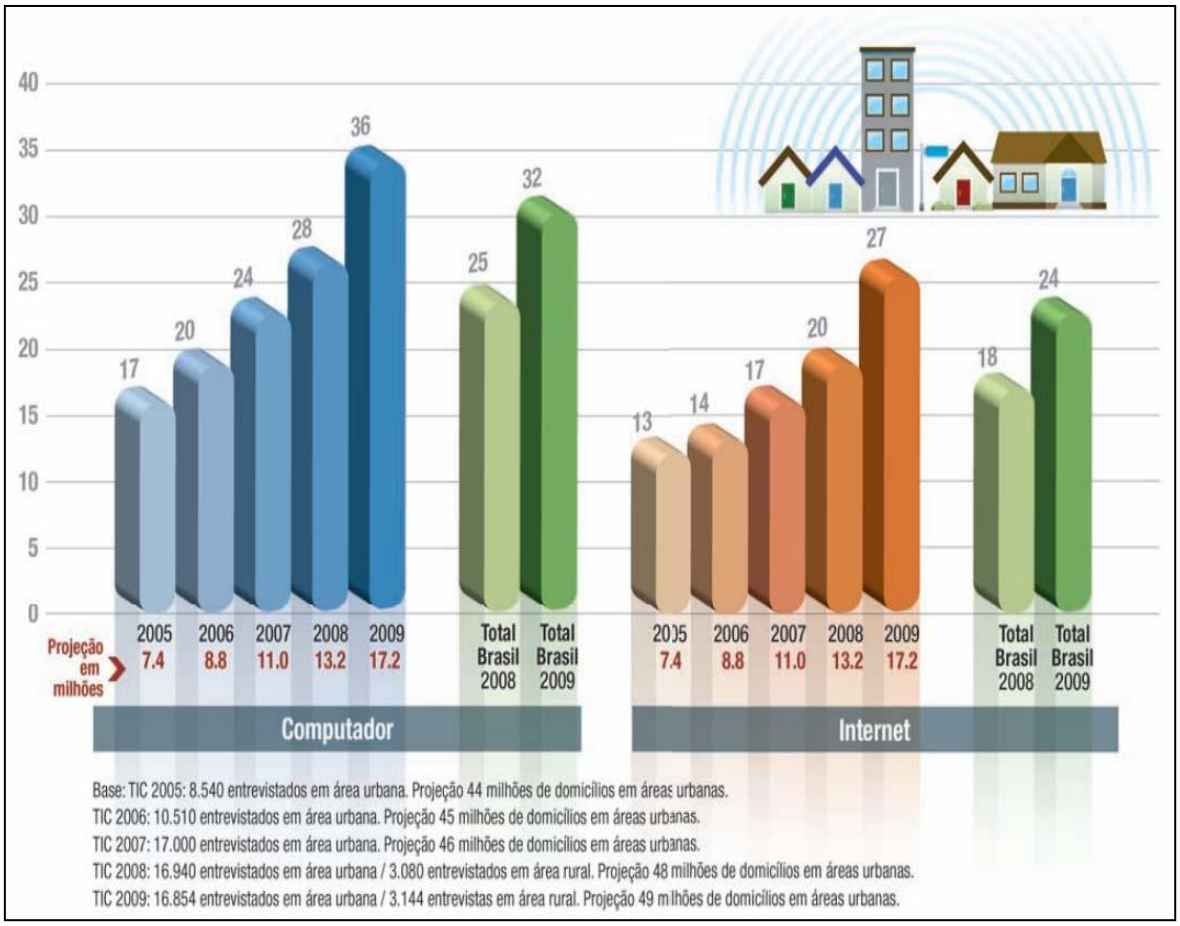

Figura 2: Computador e Internet: posse (%).
Fonte: NIC.Br (2009).

Essa maior utilização do serviço pela rede implica um aumento na sua 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."

Os autores Nakamura e Geus (2002) confirmam a influência no quesito segurança e seu peso nas organizações.

> "O conjunto de protocolos TCP/IP e a Internet possibilitaram o avanço em direção aos ambientes cooperativos, ao tornar possíveis as conexões entre diferentes organizações, de modo mais simples e mais barato que as conexões dedicadas. Porém, essa interligação teve como conseqüência uma enorme implicação quanto à proteção dos valores de cada organização."

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.

5 NIVELAMENTO DE TERMOS TÉCNICOS

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. O conhecimento sobre os protocolos apresentados neste capítulo é suficiente para o entendimento dos principais tipos de ataques e defesas sobre o *Internet Banking* que será apresentado no próximo capítulo, porém existem vários outros termos e protocolos utilizados para conexão de rede ou utilização da internet que não serão comentados neste capítulo. Os termos descritos nos próximos tópicos foram baseados em autores conhecidos e com didática simples para melhor compreensão do conhecimento de forma mais rápida e direta, suficiente para o entendimento dos principais ataques ao serviço de *Internet Banking*.

5.1 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 dos usuários de internet na tabela 2.

Tabela 2. Ordem de classificação dos usuários de internet no mundo.

Rank Order - Internet Users			
Rank	**Country**	**Internet users**	**Date of Information**
1	World	1,018,057,389	2005
2	European Union	247,000,000	2006
3	United States	208,000,000	2006
4	China	162,000,000	2007
5	Japan	87,540,000	2006
6	India	60,000,000	2005
7	Brazil	42,600,000	2006
8	Germany	38,600,000	2006

Fonte: CIA (2008).

No Brasil, o número de usuários ultrapassou os 42 milhões no ano de 2006 (IBGE, 2007). Porém esse número é pequeno em relação a países tecnologicamente mais desenvolvidos, como os Estados Unidos, por exemplo, país onde a internet foi criada.

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 em 31 de dezembro de 1958 lançar um satélite porque 1958 era o Ano Geofísico Internacional (AGI), pois nos anos geofísicos os ciclos de atividade solar estão 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 para ser lançado durante o AGI.

Em julho de 1955, a Casa Branca anunciou planos para lançar um satélite em órbita da Terra para AGI. 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 o 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 o ARPA - *Advanced Research Project Agency* em outubro do mesmo ano.

O ARPA foi criado com um único objetivo, 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. Este 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, abaixo na figura 3 do projeto original da ARPANET (TANEMBAUM, 2003).

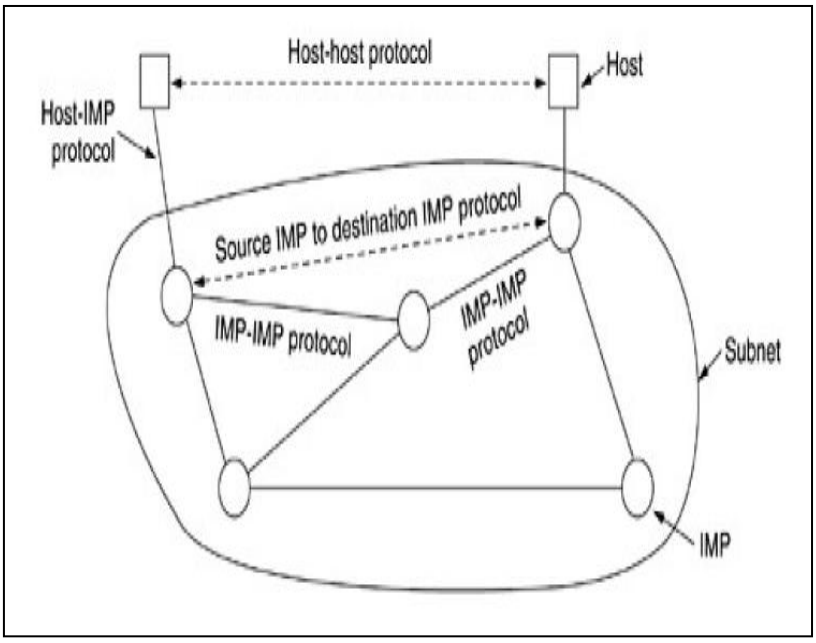

Figura 3. O projeto original da ARPANET.
Fonte: (TANENBAUM, 2003).

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, TCP/IP (*Transmission Control Protocol/ Internet Protocol)*, 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. É possível observar o crescimento da ARPANET no conjunto de imagens da figura 4 abaixo (TANEMBAUM, 2003).

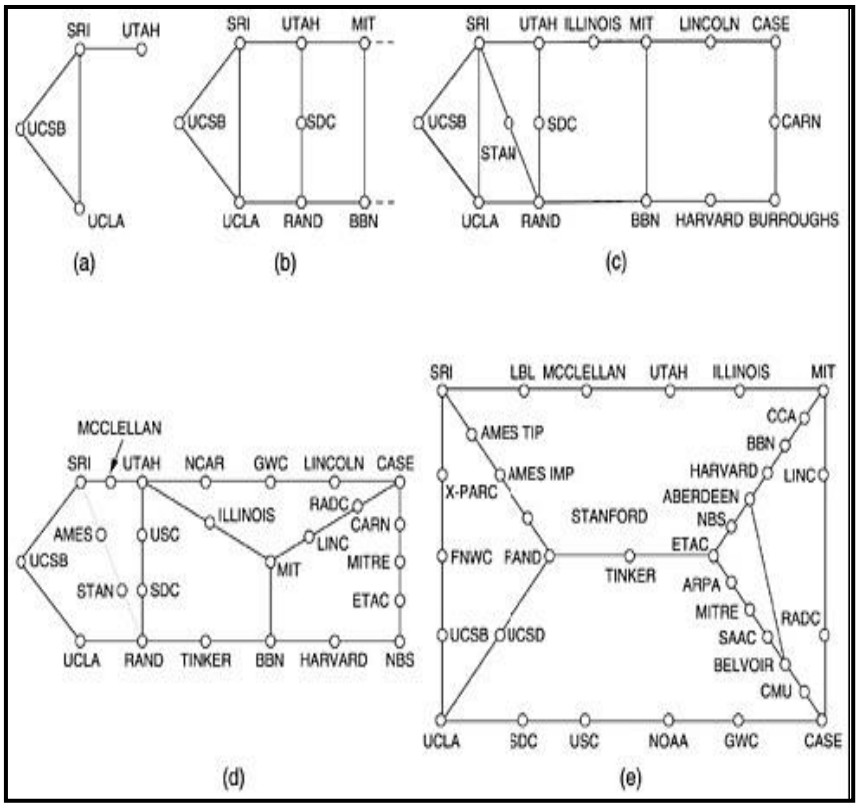

Figura 4. O crescimento da ARPANET.
Fonte: (TANENBAUM, 2003)

5.2 TCP

O TCP é o protocolo responsável pela entrega dos dados transmitidos a um endereço IP (*Internet Protocol*). 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 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.

Já existe uma 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 (UCAID - *University Corporation for Advanced Internet Development*). Devido a forma como foi idealizada a versão seis do protocolo, ela pode fornecer 340.282.366.920.938.000.000.000.000.000.000.000.000 de endereços IP únicos, seria esta a solução para a falta IP versão quatro de acordo com Morais (2009).

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

5.3 DNS

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 a necessidade de mudar os esquemas primitivos de operação da rede, sendo o DNS um dos principais agentes modificadores destas operações.

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 à 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, 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, sendo que a administração desta base de dados distribuída é delegada a varias empresas e organizações de portes diversos.

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. A figura 5 apresenta o esquema de parte da árvore da Internet.

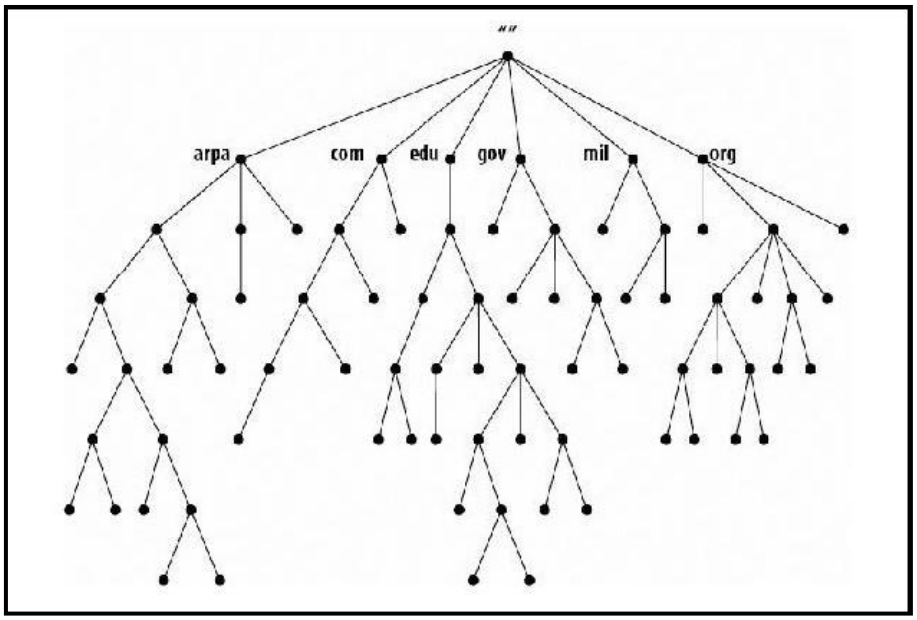

Figura 5. Representação da Árvore de DNS.
Fonte: (COSTA, 2006).

Um nome de domínio é sempre escrito seguindo um ponto mais especifico até um ponto menos especifico, de baixo para cima da arvore, domínios, até a parte menos específica, 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. A árvore de domínios do DNS é dividida em zonas. Cada zona pode conter informações de outras zonas ou hosts, veja um exemplo na figura 6.

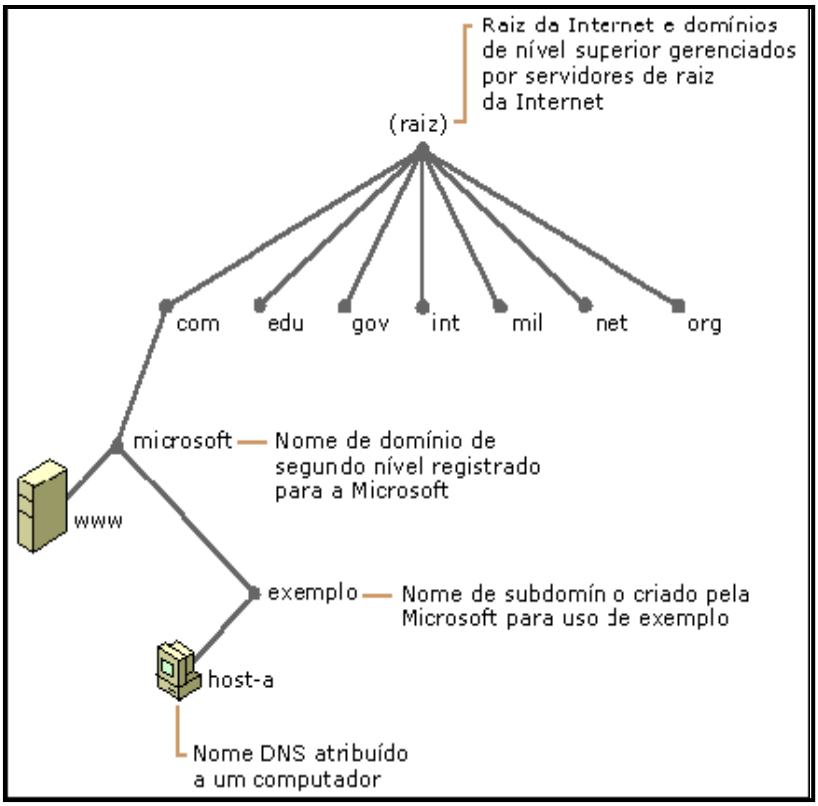

Figura 6. Hierarquia dos servidores raízes do DNS.
Fonte: (COSTA, 2006).

Os servidores DNS podem ser classificados em dois tipos principais: primário 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).

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 seriam necessários à criação de um órgão gestor da internet. 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.

5.4 HTTP

Na atual Internet o protocolo 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 é o HTTP (*HyperText Transfer Protocol*). Este protocolo especifica as mensagens que os clientes podem enviar aos servidores e que respostas eles receberão. Cada interação consiste em uma solicitação ASCII, seguida por uma resposta RFC 822 semelhante ao MIME. Os clientes e todos os servidores devem obedecer a esse protocolo, pois, ele é definido na RFC 2616.

De maneira geral um navegador entra 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 continha 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. Com elas, 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, porém ele foi criado para utilizações mais gerais que o necessário, visando futuras aplicações orientadas a objetos. Por isso, são aceitas operações chamadas métodos, diferentes da simples solicitação de uma página da Web. Cada solicitação consiste em uma ou mais linhas de texto ASCII, sendo a primeira palavra da primeira linha o nome do método solicitado. Os métodos internos estão listados na tabela 3.

Tabela 3. Os métodos internos de solicitação HTTP.

Método	Descrição
GET	Solicita a leitura de uma página da Web
HEAD	Solicita a leitura de um cabeçalho de página da Web
PUT	Solicita o armazenamento de uma página da Web
POST	Acrescenta a um recurso (por exemplo, uma página da Web)
DELETE	Remove a página da Web
TRACE	Ecoa a solicitação recebida
CONNECT	Reservado para uso futuro
OPTIONS	Consulta certas opções

Fonte: (TANENBAUM, 2003).

Para Tanembaum (2003) os nomes diferenciam letras maiúsculas de minúsculas, portanto, GET é um método válido, mas get não é. O método GET solicita ao servidor que envie a página (ou objeto, no caso mais genérico; na prática, apenas um arquivo). Das solicitações aos servidores Web a mais utilizada é método GET. A forma usual de GET é: GET nome do arquivo HTTP/1.1, onde nome do arquivo identifica o recurso a ser buscado e 1.1 é a versão do protocolo que está sendo usado.

O método HEAD solicita apenas o cabeçalho da mensagem, sem a página propriamente dita. Este método é usado para obter a data da última modificação feita na página, para reunir informações destinadas à indexação, ou apenas para testar a validade de um URL.

O método PUT é o inverso de GET: em vez de ler, ele grava a página. Esse método possibilita a criação de um conjunto de páginas da Web em um servidor remoto. O corpo da solicitação contém a página. As linhas após PUT podem incluir o cabeçalho de autenticação, para demonstrar que o chamador de fato tem permissão para executar a operação solicitada.

O método POST, que também transporta um URL, se assemelha ao método PUT, no entanto, em vez de substituir os dados existentes, os novos dados são "anexados" a ele, em um sentido mais genérico. Normalmente, nem PUT nem POST são muito utilizados hoje.

O DELETE exclui a página. Como no exemplo do método PUT, a permissão e a autenticação têm papel fundamental. Não há garantia de que o DELETE tenha sido bem-sucedido pois, mesmo que o servidor HTTP remoto esteja pronto para excluir a página, o arquivo subjacente pode ter um modo que impeça o servidor HTTP de modificá-lo ou excluí-lo.

O método TRACE serve para depuração. Ele instrui o servidor a enviar de volta a solicitação. Esse método é útil quando as solicitações não estão sendo processadas corretamente e o cliente deseja saber qual solicitação o servidor recebeu de fato.

O método CONNECT não é usado atualmente. Ele é reservado para uso futuro.

O método OPTIONS fornece um meio para que o cliente consulte o servidor sobre suas propriedades ou sobre as de um arquivo específico.

Toda solicitação obtém uma resposta que consiste em uma linha de status, possivelmente, informações adicionais. Na tabela 4 é possível observar os principais tipos de respostas. A linha de status contém um código de status de três dígitos informando se a solicitação foi atendida. O primeiro dígito é usado para dividir as respostas em cinco grupos importantes, como mostra a Figura 7. Os códigos 1xx raramente são usados Os códigos 2xx significam que a solicitação foi tratada com sucesso, e que o conteúdo (se houver) está sendo retornado. Os códigos 3xx informam ao cliente que ele deve procurar em outro lugar, usando um URL diferente ou seu próprio *cache* (conforme descreveremos mais adiante). Os códigos 4xx significam que a solicitação falhou devido a um erro do cliente, como uma solicitação inválida ou uma página inexistente. Os erros 5xx significam que o próprio servidor tem um problema, seja causado por um erro em seu código ou por uma sobrecarga temporária.

Tabela 4. Os grupos de respostas de código de status.

Código	Significado	Exemplo
1xx	Informação	100 = server agrees to handle client's request
2xx	Sucesso	200 = request succeeded; 204 = no content present
3xx	Redirecionamento	301 = page moved; 304 = cached page still valid
4xx	Erro do cliente	403 = forbidden page; 404 = page can not found
5xx	Erro do servidor	500 = internal server error; 503 = try again later

Fonte: (TANENBAUM, 2003).

A linha de solicitação pode ser seguida por linhas adicionais, elas são chamadas cabeçalhos de solicitação. As respostas também podem ter cabeçalhos, é possível verificar os mais importantes cabeçalhos na tabela 5, com esta tabela é possível observar diversos tipos de cabeçalhos, que podem ser interpretados da seguinte maneira (TANEMBAUM, 2003):

> "User-Agent que permite ao cliente informar o servidor sobre seu navegador, sistema operacional e outras propriedades. Esse cabeçalho é usado pelo cliente para munir o servidor com as informações. Os quatro cabeçalhos Accept informam ao servidor o que o cliente está disposto a aceitar na eventualidade de ele ter um repertório limitado daquilo que é aceitável. O primeiro cabeçalho especifica os tipos MIME que são bem-vindos (por exemplo, text/html). O segundo fornece o conjunto de caracteres (por exemplo, ISO-8859-5 ou Unicode-1-1). O terceiro lida com métodos de compactação (por exemplo, gzip). O quarto indica um idioma natural (por exemplo, espanhol). Se o servidor tiver uma opção de páginas, ele poderá usar essas informações para fornecer o que o cliente está procurando. Se ele for incapaz de satisfazer à solicitação, será retornado um código de erro e a solicitação falhará. O cabeçalho Host identifica o servidor. Ele é retirado do URL. Esse cabeçalho é obrigatório, ele é usado porque alguns endereços IP podem servir vários nomes DNS, e o servidor precisa ter algum meio de identificar o host a quem deve entregar a solicitação.
>
> O cabeçalho Authorization é necessário para páginas protegidas. Nesse caso, o cliente talvez tenha de provar que tem direito de ver a página solicitada. Esse cabeçalho é usado para esse caso específico. Embora os *cookies* sejam tratados na RFC 2109 e não na RFC 2616, eles também têm dois cabeçalhos. O cabeçalho *cookie* é usado por clientes para retornar ao servidor um cookie enviado anteriormente por alguma máquina no domínio do servidor.
>
> O cabeçalho Date pode ser usado em ambos os sentidos e contém a hora e a data em que a mensagem foi enviada. O cabeçalho Upgrade é usado para facilitar a transição para uma versão futura (possivelmente incompatível) do protocolo HTTP. Ele permite ao cliente anunciar o que pode admitir e permite ao servidor declarar o que está usando.
>
> Agora, vamos aos cabeçalhos usados exclusivamente pelo servidor em resposta a solicitações. O primeiro, Server, permite ao servidor saber quem ele e conhecer algumas de suas propriedades, se desejar. Os quatro cabeçalhos seguintes, todos começando com Content-, permitem ao servidor descrever propriedades da página que está enviando.
>
> O Cabeçalho Last-Modified informa quando a página foi modificada pela última vez. Esse cabeçalho desempenha uma função importante no armazenamento de páginas no cache.
>
> O cabeçalho Location é usado pelo servidor para informar ao cliente que ele deve tentar outro URL.
>
> Esse cabeçalho pode ser usado se a página tiver sido deslocada ou para permitir que vários URLs se refiram à mesma página (possívelmente em servidores distintos). Ele também é usado por empresas que têm uma página da Web principal no domínio com, mas que redirecionam os clientes para uma página nacional ou regional de acordo com seu endereço IP ou com seu idioma preferido. Se uma página for muito grande, um pequeno cliente talvez não queira recebê-la toda de uma vez.
>
> Alguns servidores aceitarão solicitações de intervalos de bytes, de forma que a página possa ser obtida em várias unidades pequenas. O cabeçalho Accept-Ranges anuncia a disposição do servidor para lidar com esse tipo de solicitação de páginas parciais.

> O segundo cabeçalho de cookie, Set-Cookie, é a forma como os servidores enviam cookies aos clientes. “Espera-se que o cliente grave o cookie e o devolva em solicitações subseqüentes ao servidor.”

Tabela 5. Alguns cabeçalhos de mensagens HTTP.

Cabeçalho	Tipo	Conteúdo
User-Agent	Solicitação	Informações sobre o navegador e sua plataforma
Accept	Solicitação	O tipo de páginas o cliente pode manipular
Accept-Charset	Solicitação	Os conjuntos de caracteres aceitáveis para o cliente
Accept-Encoding	Solicitação	As codificações de páginas que o cliente pode manipular
Accept-Language	Solicitação	Os idioma s com os quais o cliente pode lidar
Host	Solicitação	O nome DNS do servidor
Authorization	Solicitação	Uma lista das credenciais do cliente
Cookie	Solicitação	Envia um cookie definido anteriormente de volta ao servidor
Date	Ambos	Data e hora em que a mensagem foi enviada
Upgrade	Ambos	O protocolo para o qual transmissor deseja alternar
Server	Resposta	Informações sobre o servidor
Content-Encoding	Resposta	Como o cont eúdo está codificado (por exemplo, gzip)
Content-Language	Resposta	O idioma usado na página
Content-Length	Resposta	O comprimento da página em bytes
Content-Type	Resposta	O tipo MIME da página
Last-Modified	Resposta	Data e hora da última modificação na página
Location	Resposta	Um comando para o cliente enviar sua solicitação a outro lugar
Accept-Ranges	Resposta	O servidor aceitará solicitações de intervalos de bytes
Set-Cookie	Resposta	O servidor deseja que o cliente grave um cookie

Fonte: (TANENBAUM, 2003).

Um exemplo de utilização do protocolo HTTP 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 uma seqüência de comandos, é possível uma comunicação.

> “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. O log pode ser inspecionado com o uso de

> qualquer editor. Ele deve começar de maneira semelhante à listagem da Figura 7.44, a menos que a IETF tenha feito alguma alteração recente.
>
> As três primeiras linhas são a saída do programa telnet, e não do site remoto. A linha que inicializa o HTTP/1.1 é a resposta da IETF, informando que está disposta a se comunicar com você usando HTTP/1.1. Em seguida, há uma série de cabeçalhos, e depois o conteúdo. Já vimos todos os cabeçalhos, com exceção de ETag, um identificador exclusivo de página relacionado ao armazenamento no cache, e de X-Pad, um cabeçalho não padronizado e talvez um artifício para contornar bugs em algum navegador." (TANEMBAUM, 2003).

5.5 O PROTOCOLO SSL

O SSL (*Secure Sockets Layer*) é definido por garantir segurança entre as conexões. Segundo (TANEMBAUM, 2003). Quando a Web chegou ao público, no início ela foi usada apenas para distribuir páginas estáticas. Porém, 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 (*Secure Sockets Layer*) para atender a essa demanda. Esse software e seu protocolo agora também são amplamente utilizados pelo Internet Explorer

O software SSL e seu protocolo funcionam da seguinte maneira segundo Tanembaum (2003):

O protocolo SSL constrói uma conexão segura entre dois soquetes, que incluem:

1. Negociação de parâmetros entre cliente e servidor.
2. Autenticação mútua de cliente e servidor.
3. Comunicação secreta.
4. Proteção da integridade dos dados.

Vamos recorrer à tabela do modelo ISO/OSI (*International Organization for Standardization / Open System Intercinnection*) para entender o funcionamento do protocolo SSL. Observe na tabela 6 as camadas do modelo ISO/OSI. As camadas do modelo ISO/OSI representam como os dados são analisados. O modelo ISO/OSI analisa desde a camada física, onde trafegam os sinais elétricos, até a camada de aplicação na

qual o usuário tem total controle. Este modelo possui muitas vantagens da para análise e construção de uma rede sendo as principais delas (FILIPPETTI, 2002):

- Particionamento das operações de redes complexas em camadas, o que simplifica o gerenciamento;
- Possibilidade e facilidade de alteração em qualquer uma das camadas, sem a necessidade de que as outras sejam alteradas;
- Estabelecimento de um padrão de interfaces, possibilitando a interoperabilidade (*plug-and-play*) entre diversos fabricantes;
- Simplifica o ensino e o aprendizado;
- Acelera a evolução;

Tabela 6: Camadas do modelo OSI

Fonte: (CISCO, 2007).

Agora com a aplicação do protocolo SSL posicionamento tabela ISO/OSI muda, pois o protocolo SSL entra na pilha de protocolos habitual como é ilustrado na tabela 7. Observando a tabela identificamos uma nova camada colocada entre a camada de aplicação e a camada de transporte, segundo o modelo ISSO/OSI e sua tabela aceitando solicitações do navegador e enviando-as ao TCP para transmissão ao servidor. Depois que a conexão segura é estabelecida, a principal tarefa da SSL é manipular a compactação e a criptografia. Quando o HTTP é usado sobre a SSL, ele se denomina HTTPS (Secure HTTP). Às vezes, ele está disponível em uma nova porta (443), em lugar da porta padrão (8 0). O protocolo SSL não se limita ao uso apenas com navegadores da Web, porém essa é sua aplicação mais comum.

Tabela 7. Camadas para um usuário doméstico navegando com a SSL.

Aplicação (HTTP)
Segurança (SSL)
Transporte (TCP)
Rede (IP)
Enlace de dados (PPP)
Física (modem, ADSL, TV a cabo)

Fonte: (TANENBAUM, 2003).

O protocolo SSL passou por várias versões. Descreveremos apenas a versão 3, a versão mais amplamente utilizada (TANEMBAUM, 2003).

> "O SSL admite uma variedade de algoritmos e opções distintas. Essas opções incluem a presença ou a ausência de compactação, os algoritmos criptográficos a serem usados e algumas questões relativas a restrições de exportação impostas à criptografia. A última se destina principalmente a assegurar que a criptografia séria será utilizada apenas quando ambas as extremidades da conexão estiverem nos Estados Unidos. Em outros casos, as chaves serão limitadas a 40 bits, que os criptógrafos consideram uma piada. A Netscape foi forçada a colocar essa restrição para obter uma licença de exportação do governo dos Estados Unidos. A SSL consiste em dois subprotocolos, um para estabelecer uma conexão segura e outro para usar. Vamos começar examinando como as conexões seguras são estabelecidas. O subprotocolo de estabelecimento de conexões é mostrado na Figura 7. Ele começa com a mensagem 1, quando Alice envia uma solicitação a Bob para estabelecer uma conexão. A solicitação especifica a versão de SSL que Alice tem e suas preferências com relação aos algoritmos de compactação e de criptografia. Ela também contém um código RA, a ser usado mais tarde. Agora é a vez de Bob. Na mensagem 2, Bob faz uma escolha entre os diversos algoritmos que Alice pode admitir e envia seu próprio código RB. Em seguida, na mensagem 3, ele envia um certificado contendo sua chave pública. Se esse certificado não for assinado por alguma autoridade conhecida, ele também envia uma cadeia de certificados que pode ser seguida de volta até chegar a uma autoridade original. Todos os navegadores, inclusive o de Alice, são pré-carregados com cerca de 100 chaves públicas; assim, se Bob puder estabelecer uma cadeia ancorada em uma dessas chaves, Alice será capaz de verificar a chave pública de Bob. Nesse momento, Bob po de enviar algumas outras mensagens (como uma solicitação do certificado de chave pública de Alice). Ao terminar, Bob envia a mensagem 4 para dizer a Alice que agora é a vez dela.
>
> Alice responde escolhendo ao acaso uma chave pré-mestre de 384 bits e a envia para Bob, codificada com a chave pública de Bob (mensagem 5). A chave de sessão real usada para codificar os dados é derivada da chave pré-mestre combinada com ambos os códigos de modo complexo. Depois que a mensagem 5 é recebida, Alice e Bob são capazes de calcular a chave de sessão. Por essa razão, Alice informa a Bob que ele deve passar para a nova cifra (mensagem 6) e também que ela concluiu o subprotocolo de estabelecimento (mensagem 7). Bob então confirma as

mensagens de Alice (mensagens 8 e 9). Porém, embora Alice saiba quem é Bob, Bob não sabe quem é Alice (a menos que Alice tenha uma chave pública e um certificado correspondente a ela, uma situação improvável para um indivíduo).

Portanto, a primeira mensagem de Bob pode ser uma solicitação para Alice se conectar usando um nome de *login* e uma senha estabelecidos anteriormente. No entanto, o protocolo de *login* está fora do escopo da SSL. Depois que ele é realizado, por quaisquer meios, o transporte de dados pode se iniciar." (TANEMBAUM, 2003).

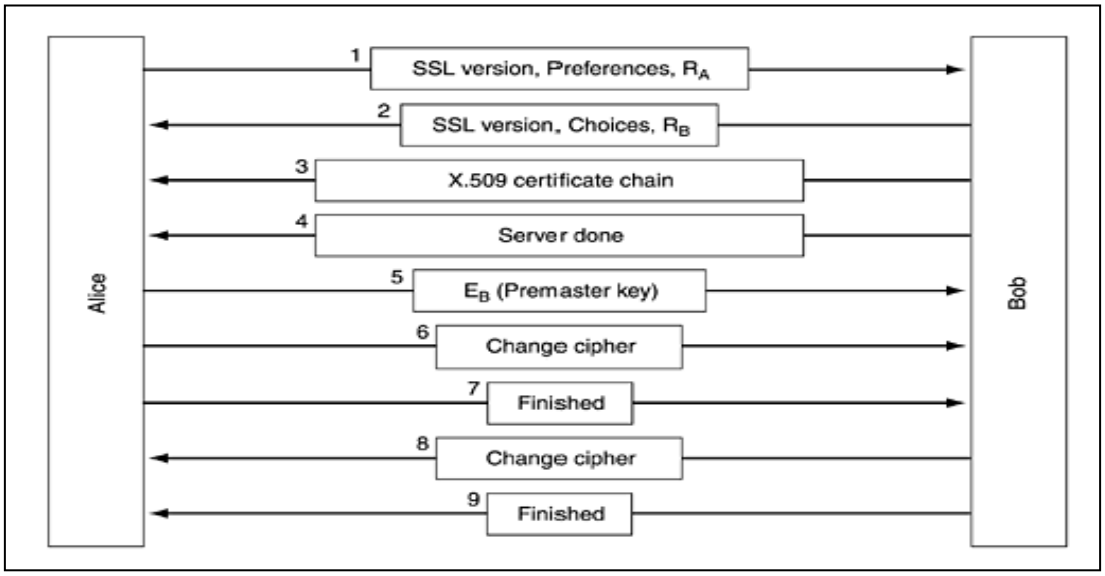

Figura 7. Versão simplificada do subprotocolo de conexões da SSL.
Fonte: (TANENBAUM, 2003).

O protocolo SSL admite vários algoritmos de criptografia (TANEMBAUM, 2003). O mais forte usa o DES triplo com três chaves separadas para criptografia e com o SHA-1, para manter a integridade das mensagens. Essa combinação é um pouco lenta, ela é normalmente usada em aplicações bancárias e outras aplicações em que a segurança deve ser maior. Para aplicações de comércio eletrônico, normalmente é usado o RC4 que utiliza uma chave de 128 bits para criptografia, e o MD5 mais comuns em autenticação de mensagens. O RC4 expande a chave de 128 bits para o seu uso. Após esse processo o algoritmo usa essa expansão para gerar um fluxo de chaves. O fluxo de chaves é submetido a uma operação lógica XOR com o texto não criptografado para fornecer a cifra de fluxo clássica como é possível observar na figura 8.

Para o transporte, é usado outro subprotocolo, como mostra a Figura 8. Primeiramente as mensagens que são de origem do navegador são divididas em unidades de 16 KB. Se a opção de compactação estiver ativada, cada unidade será compactada separadamente. Depois disso, uma chave secreta derivada dos dois códigos

e da chave pré-mestre é concatenada com o texto compactado, o resultado obtido passa por um *hash* com o algoritmo de *hash* combinado. Esse hash é anexado a cada fragmento como o MAC. O fragmento compactado somado ao MAC é então codificado com o algoritmo de criptografia simétrica estabelecido de comum acordo. Por fim, é anexado um cabeçalho de fragmento e o fragmento é transmitido pela conexão TCP (TANEMBAUM, 2003).

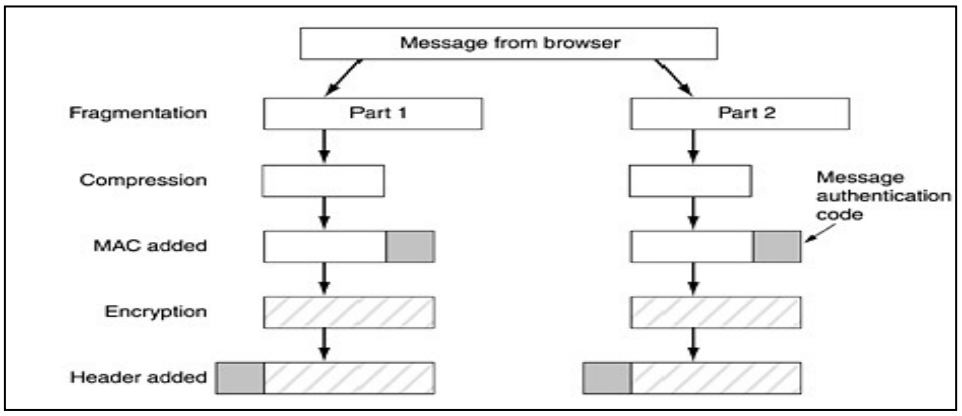

Figura 8. Transmissão de dados com a SSL.
Fonte: (TANENBAUM, 2003).

As mudanças feitas na SSL durante suas versões foram relativamente pequenas, mas suficientes para a SSL versão três e a TLS não conseguirem inter-operar. A versão da TLS também é conhecida como SSL versão 3.1 (TANEMBAUM, 2003).

Em toda conexão com a rede o usuário receberá um número de IP e ficará estabelecido um *log* de acesso, sendo possível armazenar informações no provedor de acesso como horário e tempo de conexão. Ao navegar na internet o usuário acessa outros servidores ou provedores de conteúdo, que podem ser os mesmos, como por exemplo, UOL e Terra e outros e que podem fazer, durante a conexão, *download* de arquivos (copiar dados para a estação) ou *upload* (copiar dados da estação para um provedor de conteúdo). Muitos são os termos técnicos utilizados. Contudo, com a breve apresentação das palavras e termos utilizados pretendeu-se nivelar o mínimo necessário para a compreensão de algo tão complexo (TANEMBAUM, 2003).

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

Neste capítulo serão abordados alguns tipos de ataques sobre o serviço de *Internet Banking*. As fraudes causadas pelos ataques a serviços ou instituições financeiras existem desde que os serviços foram criados e implementados. A fraude é um termo que precede o surgimento da internet, porém agora novas modalidades de fraude 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 a consumação da fraude: 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. Neste percentual existem fraudes sobre sites de comércio eletrônico, serviços de *Internet Banking*, cartas nigerianas e outras tentativas de fraude. Os valores dos prejuízos causados por estas fraudes, não são muito divulgados, alguns dados de perdas por fraudes que envolviam *Internet Banking* foram divulgadas, os prejuízos em 2005 superam os 300 milhões de reais (B2B Magazine, 2006), porém, estes valores devem aumentar cada vez mais, devido aos avanços na tecnologia e do 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 ataques que utilizam roubo de senha e os ataques que utilizam falhas de segurança em servidores DNS. Nos capítulos abaixo serão detalhados estes ataques e os principais métodos de contenção contra estes ataques.

6.1 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 suas contas bancárias para o crime) ou mesmo o pagamento de boletos pela internet.

Segundo o Ministério Público Federal (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 esta 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 os detalhamentos de como estes métodos funcionam.

6.1.2 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 esta 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 com poderosos *sniffers* (FREITAS, 2007).

6.1.3 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 à grande quantidade de pacotes em uma rede, o *sniffer* pode ser configurado para obter somente o essencial e importante: as senhas (FREITAS, 2007).

6.1.4 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).

6.1.5 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).

6.1.6 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 que ser feitas atualizando-se o próprio roteador (FREITAS, 2007).

6.1.7 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).

6.2 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 para se conseguir vantagens sobre esta pessoa enganada. Como exemplo uma pessoa que liga para o provedor e pergunta informações sobre os servidores ou senhas de usuários. Determinados 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. Esse método também pode ser utilizado para se conseguir informações sobre uma pessoa (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).

6.3 ATAQUES UTILIZANDO SERVIDORES DNS

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

6.3.1 ATAQUE UTILIZANDO PHARMING

O *pharming* é um conceito recente ao público mundial, porém ele foi um meio muito utilizado para fraude sobre o 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 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 as figura 9 para entender o funcionamento do ataque (JUSTO, 2010).

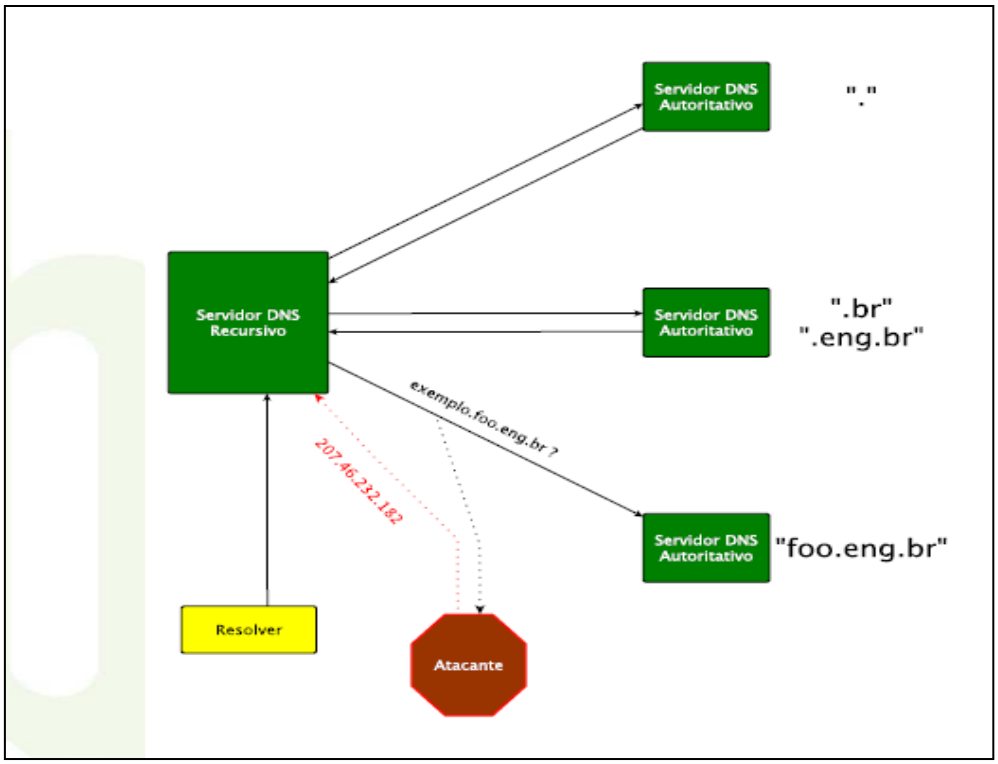

Figura 9. Poluição de cache em servidor DNS.
Fonte : (JUSTO, 2010).

A figura acima ilustra como o ataque ocorre: o atacante fornece uma informação errada sobre a resolução de um endereço e fornece essa informação ao DNS recursivo que irá entregar a informação falsa ao cliente, esta informação pode ser um IP de um site de banco falso. No próximo capítulo iremos verificar medidas de contenção contra o *pharming*, um tipo de ataque ao serviço de *Internet Banking*.

6.3.2 MEDIDAS DE CONTENÇÃO CONTRA O PHARMING

Para conter um ataque que utiliza técnicas de *pharming* pode-se 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*.

6.3.3 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 pública e privada. A chave pública é divulgada aos membros que realizam comunicação e são utilizados para a encriptação de dados (LAU, 2004). A chave privada é gerada e armazenada ao junto com ao dispositivo do usuário que é responsável pela guarda do certificado. A chave privada consegue decriptar uma mensagem encriptada pela chave pública. As figuras 10 e 11 demonstram claramente o funcionamento de chaves simétricas (JUSTO 2010).

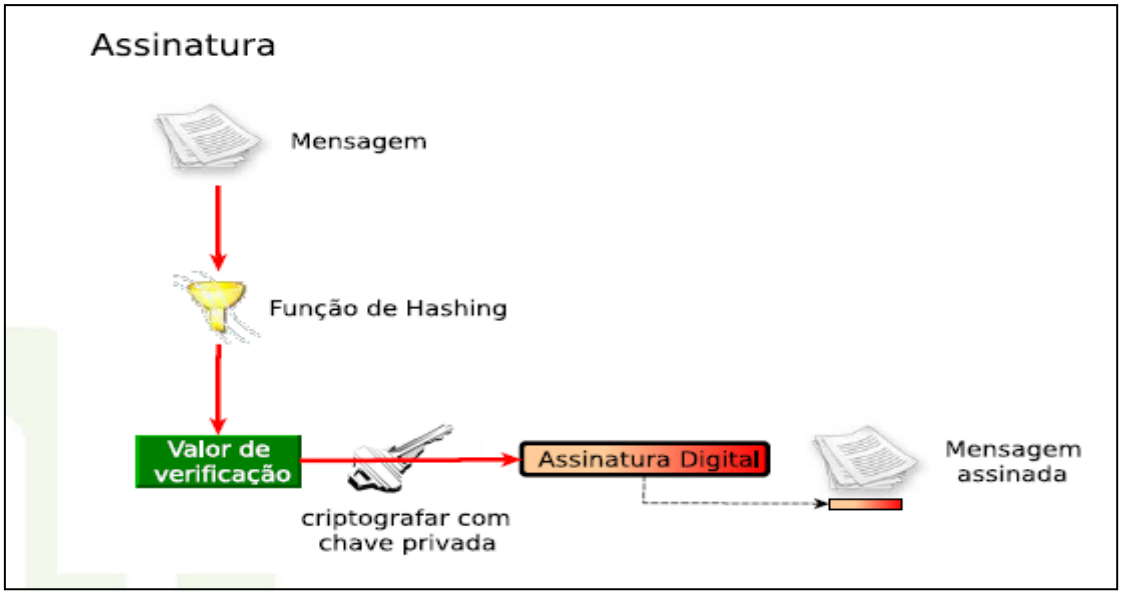

Figura 10. Chaves assimétricas assinatura.
Fonte : (JUSTO, 2010).

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).

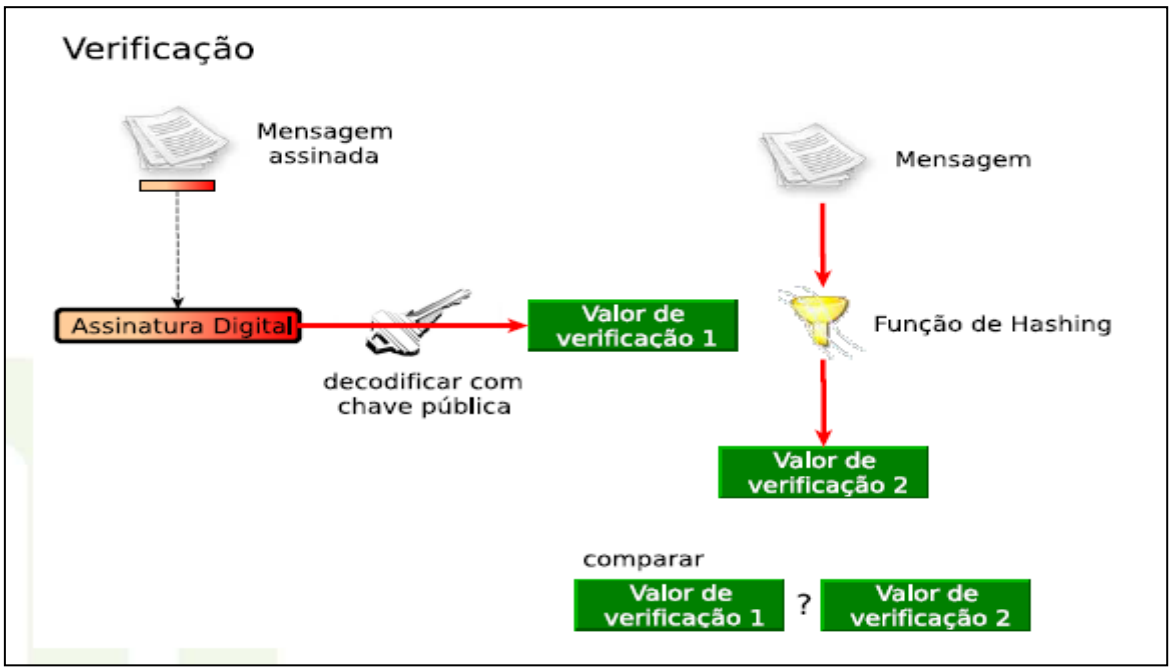

Figura 11. Chaves assimétricas verificação.
Fonte: (JUSTO, 2010).

Já a figura 11 demonstra a verificação da mensagem enviada pela origem, à mensagem é decodificada, utilizando a chave privada, após a decodificação é aplicado sobre a mensagem decriptografada o algoritmo hash, o código resultante é comparada com o código que foi enviado junto com a mensagem pela origem. Se os valores dos códigos forem iguais a mensagem pode ser considerada autentica (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 A3, faz o armazenamento do certificado em dispositivos especializados para guardar as chaves, sensíveis à temperatura, atividades sísmicas e tentativas de violação. Aos 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).

6.3.4 DNSSEC

O *DNSSEC (Domain Name System Security extensions)* 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 12 é possível observar o perímetro virtual em que o DNSSEC atua (JUSTO, 2010).

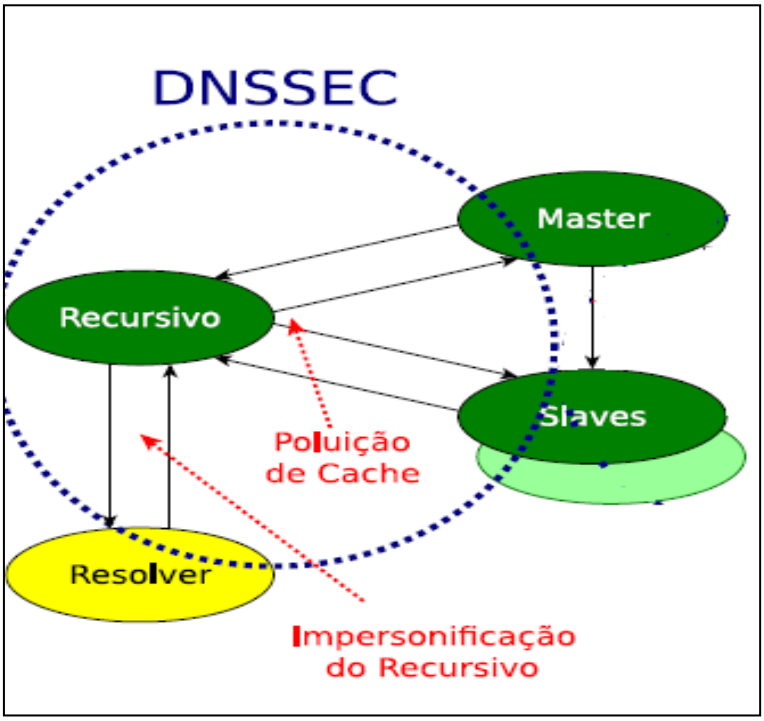

Figura 12. DNSSEC sobre o DNS recursivo.
Fonte: (JUSTO, 2010).

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 capítulo anterior e o DNS *master* ou o *slave* pode ser comparado ao destino do exemplo. Desta forma os servidores garantem autenticidade entre eles, no caso de uma tentativa de poluição de cache o servidor recursivo ira recusar as informações do atacante (JUSTO, 2010).

6.4 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).

Este cenário, sem leis especificas; e com jovens e idosos cada vez mais vulneráveis ao utilizar a Internet no Brasil só ira mudar se ocorrerem grandes modificações na sociedade brasileira. Algumas medidas já estão sendo criadas para modificar esta situação, nos últimos meses o Brasil começou um processo para conscientização de seus usuários, quem iniciou o projeto a FEBERBAN (Federação Brasileira dos Bancos) um órgão que representa várias instituições financeiras no Brasil (LOBOSCO, 2006).

No início do ano 2006 aconteceu a primeira coletiva de imprensa tendo como objetivo a orientação das fraudes junto à população. Antes deste evento, nenhuma instituição financeira tinha feito um pronunciamento oficial sobre o assunto. Iniciativas como esta da instituição FEBRABAN buscam transparência ao assunto fraude, e visa

esclarecer os clientes (principalmente os bancários) os 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 vem buscando ao mesmo tempo garantir segurança também e incentivar os usuários ao aumento no uso do serviço de *Internet Banking*, 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).

7 CONCLUSÃO

Ao término deste trabalho, reafirmam-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, as seguintes 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 internet é vantajoso, pois diminui custos, uma vez com a utilização da internet propiciam 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 internet no Brasil esta provocando um aumento no uso do serviço de *Internet Banking*. Este aumento no uso de tecnologias cada vez maior 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 até mesmo função de gerencia.

Os ataques estudados normalmente utilizam programas que analisam trafego de redes ou mesmo redirecionam informações bancarias. Algumas técnicas de engenharia social também podem ser utilizadas para as ações criminosas. Medidas para conter estes ataques já estão sendo tomadas por entidades responsáveis pela internet no Brasil e no mundo. No Brasil a entidade que representam o setor bancário, FEBRABAN, organizou palestras sobre o tema e demonstra certo interesse em divulgar o assunto. Neste trabalho ficou claro 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 a 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 está aumentando e com estes aumentos 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 internet, entre elas o *Internet Banking.*

REFERÊNCIAS BIBLIOGRÁFICAS

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

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

COMER, Douglas E. ***Internetworking with* TCP/IP**, 4ª Ed. New Jersy: 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. (Cord) **Segurança em Banco Eletrônico**. São Paulo: PricewaterhouseCoopers, 2000.

DINIZ, Eduardo H. Cinco décadas de automação. **GV–Executivo**: editorial era digital. Edição especial 50 anos. São Paulo: FGV–EAESP, 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. São Paulo: Revista dos Tribunais, v. 816, n. 10, p. 14, outubro 2003.

NEMETH, Evi.; SNYDER,Garth.;HEIN,Trent R. **Manual Completo do DNS**. Tradução Ariovaldo Griesi. Revisão técnica Mario Olimpio de Menezes. São Paulo: Pearson Makron Books, 2004.

TANENBAUM, A. C. **Redes de Computadores**. 4ª Ed. Rio de Janeiro: Campus, 2003.

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

THOMPSON, Marco Aurélio. **Invasão. BR : invasões comentadas passo-a-passo e em vídeo aulas**. 2ª 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. Disponível em <http://www.b2bmagazine.com.br/seguranca/dia-da-internet-segura>. Acesso em 15 de maio de 2011.

CENTRAL INTELLIGENCE AGENCY. Disponível em <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 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 Fevereiro de 2006.

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

DATAINTER CHANGESOFTWARE SOLUTIONS. Disponível em: <http://www.di2s.com/edi.htm>. Acesso em 03 de Abril de 2011.

EBIT EMPRESA. Disponível em: <www.ebitempresa.com.br/ index_ebitinforma.htm> . Acesso em 04 de Março de 2011.

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

IBGE. Disponível em: <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. Disponível em: <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. Disponível em: <http://www.ipv6.br/IPV6/ArtigoEsgotamentoIPv4>. Acesso em 9 de Abril de 2011.

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

O GLOBO. Disponível em: <http://oglobo.globo.com/economia/mat/2007/06/14/296 169156.asp>. Acesso em 03 de Março de 2011.

O GLOBO. Disponível em: <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. Disponível em: <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. Disponível em: <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 em: <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.

GLOSSÁRIO

Ciberespaço: termo criado pelo escritor William Gibson e inspirado no estado de transe em que ficam os adicionados de videogame durante uma partida. A palavra foi utilizada pela primeira vez no livro Neuromancer, de 1984, e adotada desde então pelos usuários da internet como sinônimo de rede.

Cyber café: (ou Ciber café) é um local que geralmente funciona como bar ou lanchonete, oferecendo a seus clientes acesso à internet, mediante o pagamento de uma taxa, usualmente cobrada por hora.

Dial-up: conecta a uma rede ou à internet usando um dispositivo que utiliza a rede telefônica. Esse dispositivo pode ser um modem que usa uma linha telefônica padrão.

Documento digital: documento codificado em dígitos binários interpretável por meio de sistema computacional. São exemplos de documentos digitais: textos, imagens fixas, imagens em movimento, gravações sonoras, mensagens de correio eletrônico, páginas web, bases de dados etc.

Domínio: é uma parte da hierarquia de nomes de computadores da internet. Um nome de domínio consiste de uma seqüência de nomes separados por ponto, por exemplo, www.folha.com.br.

Download: transferência de arquivo. Fazer download equivale a copiar determinado arquivo (texto, imagem ou programa) da internet para o computador.

FTP: protocolo para transferência de arquivos. O FTP pode ser utilizado para copiar arquivos da rede para o computador do usuário e vice versa.

HTTP: acrônimo para Hypertext Transfer Protocol (Protocolo de Transferência de Hipertexto) que permite a transferência de dados na Web.

Internauta: usuário de internet.

Lan house: estabelecimento comercial em que as pessoas podem pagar para utilizar um computador com acesso à internet e a uma rede local.

Offline: desconectado com a unidade de processamento central de um computador; comunicação offline – indireta.

Online: em ligação direta com a unidade de processamento central de um computador.

Provedor de acesso: varejista de conectividade à internet. Ligado a um provedor de backbone, revende conexão à internet aos usuários finais.

Provedor de conteúdo: empreendimento que disponibiliza informações na rede para os 80 usuários.

Proxy: um servidor posicionado entre um cliente e o servidor real, onde estão os dados. Esses servidores têm uma série de usos, como filtrar conteúdo, providenciar anonimato, entre outros.

Servidor: computador que armazena páginas da web.

Spam: abreviação em inglês de spiced ham (presunto condimentado), utilizado na acepção de mensagem eletrônica não solicitada enviada em massa.

Telecentros: espaço público onde as pessoas podem acessar microcomputadores, conectarem a internet, jogar, etc.

Upload: transferência de dados de um computador local para um servidor.

Web: Abreviatura para designar o World Wide Web. É a rede mundial de computadores.

WWW: World Wide Web. Literalmente, teia de alcance mundial. Consiste em software cliente/servidor. A WWW utiliza o HTTP para trocar documentos e imagens. É por meio da WWW que se acessa a grande parte da informação disponível na internet.