UNIVERSIDADE GUARULHOS

GILBERTO PINTO

ESTUDO DOS ASPECTOS DE SEGURANÇA ENVOLVIDOS NO COMÉRCIO ELETRÔNICO: UMA ABORDAGEM AO PROTOCOLO HTTPS

GUARULHOS

2002

GILBERTO PINTO

ESTUDO DOS ASPECTOS DE SEGURANÇA ENVOLVIDOS NO COMÉRCIO ELETRÔNICO: UMA ABORDAGEM AO PROTOCOLO HTTPS

Dissertação apresentada como exigência parcial para obtenção do grau de Mestre em Ciência da Computação à Comissão Julgadora da Universidade de Guarulhos, sob a orientação do Prof. Dr. José Roberto Bollis Gimenez.

UNIVERSIDADE GUARULHOS
GUARULHOS - 2002

1º Examinador_____

2º Examinador_____

3º Examinador_____
(orientador)

A minha esposa Regina e ao meu filho Gustavo pelo apoio dado e pela paciência demonstrada durante a execução desta dissertação.
Aos meus pais Flávio e Vilma que me encaminharam na trilha do saber.

RESUMO

O crescimento e a popularização da Internet permitiu que o comércio eletrônico, que anteriormente se limitava a aplicações de EDI e EFT, se disseminasse pela rede atingindo um número de pessoas nunca imaginados.

A Internet passou a ser tratada como um segmento de mercado para um grande número de empresas da atualidade e passou a fazer parte das estratégias de negócios destas empresas, movimentando bilhões de dólares por todo o mundo.

Este mercado gigantesco está em constante evolução e permite vislumbrar um crescimento ainda longe do seu limiar.

Porém, se as perspectivas de negócios são boas, temos ainda um lado obscuro da rede que lança uma série de ameaças às empresas e aos usuários da Internet.

Estas ameaças muitas vezes são difundidas na mídia amedrontando usuários da rede, que sentem-se inseguros ao disponibilizar informações sigilosas, como número de cartões de crédito ou senhas bancárias. Desta forma, estas ameaças tornam-se um obstáculo para o desenvolvimento do comércio eletrônico.

Esta dissertação se propõe a discutir o comércio eletrônico, as ameaças que a Internet representa e as ferramentas de segurança que se contrapõem as estas ameaças, possibilitando assim, o uso seguro da Internet como meio para o comércio eletrônico.

ABSTRACT

The Internet growth and popularity enabled electronic commerce, early limited only to EDI and EFT applications, to be scattered to the net, reaching an amount of people never wondered.

The Internet turned into a market partition for many companies at the present time and became an business strategy for these companies, which moves billion dollars around the world.

The huge market is continuously expanding and it inferable that figure inflexion point is far from its verge.

However, whether the business viewpoint seems to be good, there is a dark side on the net, which causes threats to these companies and the Internet user.

These threats are, sometimes spread in the media, frightening the net users, who feel insecure on sending their confidential information, like a credit card numbers or bank passwords. These threats turn out to be an obstacle to the electronic commerce development.

This dissertation proposes to discuss the electronic commerce , the threats Internet presented by Internet and the security tools to prevent such this threats, allowing a secure environment for the electronic commerce.

AGRADECIMENTOS

Ao Professor Doutor José Roberto Bollis Gimenez, pela condução da dissertação e pelo apoio dado nos momentos de incerteza.

LISTA DE TABELAS

LISTA DE FIGURAS

FIGURAS (CAP. 7) *PÁGS.*

FIGURAS (CAP. 8) *PÁGS*

SUMÁRIO

INTRODUÇÃO

A Internet e o comércio eletrônico.

A Internet que há pouco tempo atrás estava restrita a ambientes acadêmicos, se expandiu de forma avassaladora. Este crescimento ocorreu no número de usuários, sites existentes, quantidade de serviços e na informação disponível.

Alguns termos como: “navegar na Internet”, que designa o fato de uma pessoa acessar diferentes home pages, ou ainda, “internauta” que define a pessoa que está “navegando”, passou a fazer parte do vocabulário de uma boa parte da população e podem ser encontrados em dicionários, como o conceituado Dicionário Aurélio.

Existem pessoas que mal se lembram de como eram suas vidas antes do email (correio eletrônico) e do uso da Internet e sua variada gama de recursos e serviços.

Dentre os serviços oferecidos através da Internet, pode-se destacar os classificados como “comércio eletrônico”. Por sua praticidade para o usuário e por ser um novo segmento de mercado para as empresas, o comércio eletrônico se tornou alvo de grandes investimentos e de grandes campanhas publicitárias, que visam ampliá-lo cada vez mais.

A tendência é que o comércio eletrônico em seus variados conceitos, cresça cada vez mais, abrangendo um número maior de empresas e de consumidores, movimentando cifras astronômicas.

Formulação da situação problema.

Há uma perspectiva de crescimento quase sem limites do comércio eletrônico e um otimismo muito grande em relação aos valores transacionados através deste sistema.

Porém, a Internet, como meio de comunicação que massifica e que viabiliza o comércio eletrônico, não é um ambiente reconhecidamente seguro, estando sujeito à várias ameaças.

Estas ameaças partem de usuários da Internet especializados em violar transmissões de dados, desfigurar home pages ou ainda, obter dados indevidos. Estas práticas são implementadas através das mais variadas técnicas de ataques.

Estes usuários, genericamente denominados hackers, podem se aproveitar de falhas dos sistemas ou descuidos dos usuários, para praticar seus atos ilícitos através da Internet, pondo assim em xeque a viabilidade do comércio eletrônico.

Objetivos do estudo.

Os objetivos desta dissertação são :

- Estudar a viabilidade do comércio eletrônico, estritamente do ponto de vista da segurança dos dados.
- Buscar as causas da insegurança, que remonta à origem da própria Internet.
- Verificar quais garantias devem existir para o comércio eletrônico ser considerado seguro.

- Analisar os riscos para estas garantias, ou seja, quais ações que podem trazer insegurança para o comércio eletrônico.
- Estudar os conceitos que visam implementar segurança às transmissões de dados e, principalmente, quais as ferramentas existentes baseadas nestes conceitos.
- Mostrar as opções disponíveis para empresas que queiram disponibilizar sites de comércio eletrônico, contando com o apoio de empresas especialistas em hospedagem segura de sites.

Estrutura da dissertação.

Capítulo 1 – A Internet. Neste capítulo será demonstrado um breve histórico da Internet, para que se possa estudar a sua formação e o seu funcionamento básico, demonstrando assim as origens da insegurança na rede.

Capítulo 2 – O comércio eletrônico. Neste capítulo serão determinadas as formas de comércio eletrônico e as expectativas de crescimento deste setor.

Capítulo 3 – Segurança na Internet e o comércio eletrônico. Este capítulo aborda alguns usuários da rede, que valem-se de seus conhecimentos para agir de má fé, e como estas ações podem afetar o comércio eletrônico.

Capítulo 4 – Garantias necessárias ao comércio eletrônico. Neste capítulo são apresentadas as garantias que devem existir para que o comércio eletrônico possa ser considerado seguro.

Capítulo 5 – Principais riscos à segurança dos dados na Internet. Neste capítulo são abordados os riscos que se contrapõem as garantias necessárias. São demonstradas também, algumas das principais formas de ataque existentes.

Capítulo 6 – Fundamentos de segurança na transmissão de dados. Neste capítulo são estudados os principais fundamentos que visam trazer segurança à transmissão de dados na Internet. Dentre estes podemos destacar a criptografia.

Capítulo 7 – Ferramentas para implementar segurança na transmissão de dados. Com base nos fundamentos estudados no capítulo VI, são demonstradas neste capítulo as ferramentas que visam proporcionar segurança à Internet.

Capítulo 8 – O uso do protocolo HTTPS como ferramenta de segurança na transmissão de dados. Este capítulo é dedicado exclusivamente ao protocolo HTTPS, dada sua importância e popularidade.

Capitulo 9 – Hospedagem segura. Neste capítulo são apresentados os serviços de hospedagem (hosting), que permitem às empresas sem uma grande infra-estrutura de informática, disporem de um site de comércio eletrônico.

Conclusão. Discute os pontos mais importantes e enfatiza os objetivos atingidos com o trabalho.

Bibliografia. Livros, dissertações, textos eletrônicos, revistas, jornais e periódicos científicos que são citados ao longo do trabalho.

Bibliografia complementar. Livros, dissertações, textos eletrônicos, revistas, jornais e periódicos científicos que não são citados ao longo do trabalho, mas que ajudaram a embasar e a nortear o raciocínio do trabalho.

CAPÍTULO 1

Internet

Este capítulo faz um histórico da Internet, desde o seu surgimento para fins militares, passando pelo uso de universidades e pesquisadores, até o uso em larga escala no mundo todo, mostrando seus principais padrões e definições. A importância deste capítulo está no fato desta dissertação estar abordando a Internet como meio principal para transmissão dos dados.

1.1 – A ARPANET.

Na década de 60 durante a guerra fria foi desenvolvida nos Estados Unidos uma rede de comunicação que pudesse se manter ativa durante um possível ataque nuclear. Todo o projeto foi subvencionado pela ARPA (Advanced Research Projects Agency), uma divisão científica do Pentágono (Centro militar norte-americano).

A rede foi baseada no conceito que cada nó deveria conter um host (computador ligado à rede) e que se um desses nós ficasse desativado, os pacotes poderiam ser roteados por caminhos alternativos e mesmo assim chegar ao seu destinatário. Este conceito se baseava no modelo de rede proposto por Paul Baran em 1962.

Baran era pesquisador da Rand Corporation [1] uma empresa técnica de utilidade pública, ligada a Força Aérea Americana.

O estudo de Baran [2] sobre redes distribuídas e comutação de pacotes foi portanto, financiado pela Força aérea dos EUA, que tinha interesse em desenvolver uma rede de comunicação resistente a ataques nucleares.

Uma conseqüência importante desta escolha e dos desenvolvimentos posteriores é que a rede Internet herdou esta característica. Isto implica que qualquer defeito em equipamentos da rede não significa que ela pare de funcionar, como sequer chega a interromper as comunicações entre os processos no momento que o problema ocorre, desde que se mantenha alguma conexão entre os processos citados, resultando desta forma, numa rede robusta.

Em dezembro de 1969, finalmente a rede da ARPA entrou no ar, em fase experimental, e ficou conhecida como ARPANET. Esta rede ligava 4 diferentes hosts, inclusive conectando computadores de diferentes configurações da Universidade da Califórnia em Los Angeles, Universidade da Califórnia em Santa Bárbara, Universidade de Utah e o Stanford Research Institute [3].

A rede original interligava a comunidade acadêmica e a comunidade militar americana, se expandindo rapidamente e passando a incluir diferentes plataformas, seja do ponto de vista do hardware ou do software utilizado, tornando possível a comunicação entre sistemas variados de diferentes concepções.

Rapidamente a rede cresceu. Em pouco menos de 3 anos, em Setembro de 1972, a rede já conectava todo território norte-americano.

O crescimento da ARPANET levou ao desenvolvimento de um novo protocolo de comunicação específico inter-redes, que foi denominado TCP/IP. A ARPANET continuou crescendo e ao sistema de endereçamento dos hosts foi adaptado o DNS (Domain Naming System) que teve por objetivo organizar as máquinas em domínios, mapeando o nome dos hosts para os endereços IP correspondentes.

O DNS é utilizado para mapear nomes de hosts e destinos de mensagens de correio eletrônico em endereços IP, ele será melhor explicado no item 1.6.2, pois tal recurso é um dos pilares da Internet atualmente.

1.2 – CSNET.

O crescimento e o sucesso da Arpanet, fez nascer a Csnet, que teve por objetivo interligar os Departamentos de Ciência da Computação dos E.U.A.

Para participar da rede da ARPA era necessário a existência de um convênio entre a universidade interessada e o DoD (Department of Defense) americano, o que inviabilizava a entrada de muitas instituições interessadas na adesão.

A partir da idéia liderada pela Universidade de Wisconsin e com o apoio da ARPA e da NSF (National Science Foundation) a rede Csnet tornou-se operacional em Julho de 1982. Apesar de pobre em relação a rede da ARPA, pois contava apenas com serviço de correio eletrônico e troca de arquivos, algumas de suas características influenciaram todo o desenvolvimento da área, sendo que, entre estas, podemos citar :

- A Csnet juntamente com a Arpanet podem ser consideradas precursoras da Internet.

- O desenvolvimento da rede contou com a adesão de toda a comunidade de pesquisa em computação, o que significou algumas milhares de pessoas trabalhando de forma cooperativa, mesmo que em plataformas

de computadores diferentes, estabelecendo novos protocolos de comunicação para isto.

- Houve amplo envolvimento da NSF, financiando e administrando o funcionamento da rede.

1.3 – A USENET.

A outra rede que deve ser citada é a USENET, que surgiu por volta de 1978 com o intuito de permitir a troca de informação entre seus usuários. Idealizada por Tom Truscott e Jim Ellis, utilizava um recurso bastante simples, baseado num computador que tivesse o sistema operacional UNIX, um modem e uma linha discada para conexão.

A rede dispunha apenas da troca de arquivos e do correio eletrônico, que era realizado por um programa incluído no próprio sistema UNIX.

Alguns fatos merecem ser citados :

- A USENET cresceu descentralizada e sem a necessidade de um financiamento

- A rede chegou a contar com centenas de milhares de usuários.

- A sua arquitetura serviu de modelo para a formação de uma das primeiras redes européias a EUNET.

1.4 – A NSFNET.

No ano de 1984 a NSF iniciou o desenvolvimento de uma nova rede de alta velocidade, com o objetivo de suceder a ARPANET.

A rede contava com seis centrais de supercomputadores e com mais 20 redes regionais conectadas à rede de supercomputadores, e tinha o objetivo de fomentar o acesso ao meio acadêmico, científico e cultural.

A rede ficou conhecida como NSFNET. Também utilizou o TCP/IP como protocolo básico e logo se tornou um sucesso entre seus usuários.

A NSFNET determinava que o uso de sua rede deveria ser aplicado estritamente à pesquisa e à educação, regulamentada através da AUP – Acceptable Use Policy.

Este fato influenciou o crescimento de redes privadas e competitivas, as quais foram financiadas com objetivos comerciais. Esta política prosseguiu até 1995, quando houve o fim do subsídio da NSFNET. A verba recuperada foi distribuída de forma competitiva, para que as redes regionais pudessem ter conectividade em todo território americano.

A privatização da NSFNET permitiu que o backbone passasse a ser distribuído e complexo, sendo formado por múltiplas redes de prestadores de serviços em telecomunicações, como AT&T, MCI, Sprint e outros. A rede deixou de ter um backbone central e passou a ter um conjunto de provedores de acesso. Isto também representou a possibilidade da rede permitir o tráfego de informações comerciais.

1.5 – A Internet.

O número de redes, máquinas e usuários conectados à ARPANET cresceu rapidamente e quando a NSFNET e a ARPANET foram interconectadas, este crescimento tornou-se exponencial [4].

A rede foi conectada a outras redes existentes no Canadá, Europa e Pacífico; este conjunto de redes, ou inter-redes passou a ser denominado INTERNET (Interconnected Networks). A Internet nada mais é portanto que uma megarede resultante natural da ARPANET e da NSFNET.

A Internet não tem oficialmente um órgão responsável. O que existe é o controle de padronização e recomendações através do IAB (Internet Architecture Board), que gerencia as definições de padrões de protocolos, criação de novos protocolos, evolução, etc.

O IAB é um fórum mantido pela ISOC (Internet Society) [5]. O controle operacional da Internet é realizado por diversos órgãos, inclusive internos em diferentes países. Podemos citar alguns exemplos:

- IANA (Internet Assigned Numbers Authority), órgão responsável por toda política de fornecimento de endereços IP.

- InterNIC (Internet Network Information Center), órgão responsável pela distribuição de endereços IP no âmbito das Américas, assim como dos domínios (DNS).

- GTLD-Mou, comitê criado em 1997 para decidir sobre a padronização de novos nomes básicos na Internet. Exemplo: .com, .edu, .gov, etc.

- IETF (Internet Engineering Task Force), órgão executivo do IAB, responsável pela definição e padronização dos protocolos utilizados na Internet.

- IRTF (Internet Research Task Force), órgão responsável por criar, projetar e propor novas aplicações ao IAB.

Nos diversos países, existem órgãos específicos para o controle da Internet local. No Brasil, o órgão responsável pela definição de políticas de utilização é o Comitê Gestor da Internet [6], sendo o Registro.br a entidade responsável pelo registro e manutenção em nomes de domínio no Brasil, de acordo com as normas estabelecidas pelo Comitê Gestor.

No início, em 1989, a Internet no Brasil [7] se resumia ao uso de instituições acadêmicas como a FAPESP, USP, UNICAMP, PUC-Rio, UFRJ e outras. Foram formados dois backbones regionais, a RedeRio e a ANSP (Academic Network at São Paulo) interligando as principais instituições destes estados. Posteriormente foi criada a RNP (Rede Nacional de Pesquisas) com o objetivo de formar um backbone nacional de acesso à Internet e de estimular a formação das redes regionais como a Rede Minas, Rede Tchê e outras.

Em 1995, foi liberado o tráfego para atividades comerciais, com a Embratel montando e operando o backbone comercial no Brasil. O fornecimento de acesso à

Internet não foi considerado monopólio estatal, permitindo o surgimento de provedores de acesso à Internet.

1.6 – Conceitos básicos da Internet.

Apesar de toda a anarquia que existe na Internet, aliás desde os seus primórdios, podemos identificar, alguns conceitos básicos que norteiam a sua existência :

1.6.1 – Protocolo TCP/IP.

O protocolo TCP/IP (Transmission Control Protocol / Internet Protocol) é um conjunto de protocolos que podem ser utilizados sobre qualquer estrutura de redes, desde uma simples conexão entre duas máquinas, como uma rede complexa (rede de pacotes). Ele é suportado por redes do tipo Ethernet, Token-Ring, FDDi, PPP, ATM, X.25, Frame-Relay e se adapta a diversos meios físicos, como satélites ou linha discada.

Considerando o modelo OSI, o TCP/IP também utiliza o conceito de camadas, sendo estas: Aplicação, Transporte, Inter-rede e Rede.

Camada de Rede: Também denominada Host/Rede. Esta camada é responsável pela transmissão dos datagramas, que são gerados na camada Inter-rede, realizando o mapeamento de endereços da camada inter-rede para o endereço da rede.

Os principais protocolos suportados nesta camada são: Ethernet, PPP, Token-Ring, FDDI, HDLC, SLIP, X.25, Frame Relay, ATM, etc.

Camada Inter-Rede: Responsável pela comunicação entre as máquinas através do protocolo IP. O reconhecimento de cada máquina é realizado pelo identificador denominado endereço IP.

O protocolo IP realiza a função mais importante da camada, que é a própria comunicação inter-redes, através do roteamento, que designa a função de transportar as mensagens entre as redes e de decidir qual será o caminho na rede para que a mensagem chegue ao destino.

Camada de Transporte: Responsável por manter a conversação entre a origem e o destino da mensagem, sem levar em conta os demais níveis.

Nesta camada são utilizados dois protocolos: O UDP (User Datagram Protocol), ou o TCP (Transmition Control Protocol), conforme requisitar a aplicação.

O UDP caracteriza-se por ser um protocolo sem conexão, não confiável. Por estes motivos, é mais utilizado em aplicações onde a velocidade da entrega dos dados é mais importante do que a qualidade com que os dados são entregues.

O TCP caracteriza-se por ser um protocolo com conexão confiável, para permitir que os dados sejam entregues sem erro. O TCP controla o fluxo da informação, o controle de erros de transmissão, a sequenciação e a multiplexação dos dados.

Camada de Aplicação: Contém os protocolos básicos, que são responsáveis pelo sistema de comunicação do TCP/IP, como o DNS, ou pelos protocolos que

fornecem os serviços para os usuários, entre os quais podemos citar: FTP, HTTP, Telnet, SMTP, POP3, Gopher, etc.

Estas camadas podem ser demonstradas através da figura 1.1 :

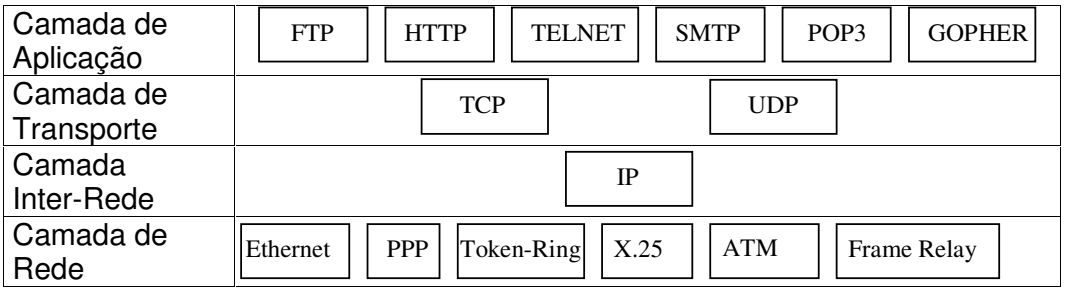

Figura 1.1 : O protocolo TCP/IP

O protocolo TCP/IP tornou-se um padrão na Internet. Segundo Comer: *"Um computador conectado a Internet necessita de ambos protocolos (TCP e IP). O IP possibilita a transferência dos pacotes entre a origem e o destino, mas não trata de problemas como datagramas perdidos ou entregues fora de ordem. O TCP trata estes problemas, portanto, juntos estes protocolos permitem a transmissão de dados na Internet"* [8]

1.6.2 – URL (Uniform Resource Locator).

O URL (Localizador Universal de Recurso) é usado para endereçar uma página na Internet. Para se localizar uma página na Internet, existem 3 perguntas que devem ser respondidas, segundo Tanenbaum [4]:

1 – Qual o nome da página?

2 – Onde a página está localizada?

3 – Como a página pode ser acessada?

O URL possui três partes que respondem estas perguntas:

1 - O protocolo da aplicação, também denominado esquema de acesso, responde a 3ª questão (Como a página pode ser acessada?). Isto significa dizer que a primeira parte do URL estabelece qual protocolo de comunicação será utilizado para se comunicar com a página endereçada.

Normalmente o protocolo mais comum de uso na Internet é o HTTP, porém existem outros protocolos como: Gopher, File, News, Telnet, Ftp e Mailto, sendo que destacam-se entre estes, pela popularidade, o protocolo FTP, utilizado para transferência de arquivos e o protocolo MAILTO para troca de e-mail.

2 - O nome do domínio, que responde a 2ª questão (Onde a página está localizada?), ou seja, o nome DNS da máquina em que a página está localizada.

Cada host ligado à Internet tem um endereço único, numérico e que difere de qualquer outro host. Este endereço é denominado endereço IP.

O DNS é utilizado para que a partir de um domínio registrado se possa obter o endereço IP da máquina, para que a conexão TCP possa ser definitivamente estabelecida. O DNS é, portanto, um mapeamento entre endereços IP e nomes (domínios).

O sistema utilizado tem o objetivo de ser escalável, suportando a definição de nomes únicos para todas as redes e máquinas na Internet e permitir que a administração do serviço seja descentralizada.

A estrutura de nomes tem o formato de uma árvore invertida onde a raiz não possui nome. Os ramos imediatamente inferiores à raiz são denominados TLDs (Top-Level Domain Names), entre os quais podemos citar : .com, .edu, .org, .net, .br, etc. Os TLDs que não designam países são mais utilizados nos EUA; os demais países utilizam a sua própria designação para a classificação interna.

Como exemplo podemos citar o Brasil, onde temos os nomes: .com.br, .gov.br, .net.br, etc. Os GTLDs (Generic Top Level Domains Names), principais domínios genéricos, são administrados pelo InterNIC .

Os domínios são independentes das redes, não existindo nenhum relacionamento entre eles. O DNS possui uma estrutura inversa para poder representar o endereçamento da rede, fazendo o mapeamento do endereço IP a partir do domínio estabelecido.

3 - O nome da página, que responde a 1ª questão (Qual o nome da página?), ou seja, especifica o nome do arquivo (página) que se deseja acessar, dentro da máquina localizada.

Podemos exemplificar com um dos endereços utilizados nesta pesquisa : *http://www.revista.unicamp.br/infotec/admsis/admsis8-1.html.* Neste caso o protocolo está especificado como *http*, o domínio utilizado é *www.revista.unicamp.br*, a terceira e última parte, estabelece o path */infotec/admsis/* e o nome do arquivo acessado *admsis8-1.html*.

Como podemos ver, o URL responde às três perguntas de trás para frente, primeiro estabelecendo o protocolo, depois o domínio (DNS) e por último o nome do arquivo propriamente pesquisado.

1.6.3 – HTTP (Hiper Text Transfer Protocol).

O HTTP é o protocolo padrão da Web, ele é composto basicamente de dois momentos distintos: Um conjunto de solicitações do browser ao servidor e um conjunto de respostas que retornam do servidor ao browser.

O protocolo HTTP foi desenvolvido para ser utilizado na Internet, embora seu desenho definitivo permite que ele possa ser usado em outras formas de aplicação.

Quanto à forma de transporte, o uso mais comum é em conjunto com o TCP, embora não seja a única forma possível.

1.6.4 – Markup Languages.

A classe conhecida como “Markup Languages” (linguagens de marcação) em especial o HTML (Hiper Text Markup Language) se tornou um dos principais padrões para desenvolvimento de páginas na Internet.

O HTML é uma linguagem que obedece ao padrão SGML (Standard Generalized Markup Language). Ele tornou-se padrão para desenvolvimento de páginas na Internet, permitindo que seus usuários criem páginas com textos, elementos gráficos, sons e ponteiros para outras páginas.

O HTML é uma linguagem de marcação, isto é, os comandos de formatação do texto estão embutidos no próprio texto. Estes comandos definem a estrutura da página, os caracteres utilizados e os hiperlinks existentes.

Desta forma, é mais fácil a padronização dos diferentes browsers, pois com a marcação no próprio texto, o browser pode interpretar o comando e formatar a página de acordo com seu próprio padrão de fontes ou de ambiente.

O HTML é um arquivo texto, com a extensão .HTM, ou .HTML. Ele pode ser gerado por programas específicos, onde o produtor da página web desenha a página no formato desejado e o programa gera então o fonte HTML.

Outra linguagem que também se tornou popular na Internet é o XML (eXtensible Markup Language) [9]. Mais poderosa que o HTML o XML teve seu uso disseminado nos anos mais recentes. O XML também obedece o padrão SGML,

porém com mais recursos que o HTML. Através do XML é possível, por exemplo, montar uma página dinamicamente a partir de uma consulta a um banco de dados, permitindo a interface com o usuário.

1.7 – WWW - World Wide Web.

Até o início da década de 1990, a Internet era utilizada basicamente por pesquisadores de universidades ou pesquisadores do governo. Os serviços disponíveis eram o correio eletrônico, o serviço de News e o login remoto.

A partir do aparecimento da aplicação WWW (World Wide Web) esta realidade foi modificada e a Internet passou rapidamente a contar com milhões de usuários.

As aplicações WWW surgiram no início da década de 90, no meio científico para permitir que documentos do Centro Europeu de Pesquisa Nuclear (CERN) pudessem ser rapidamente distribuídos entre os cientistas da instituição.

A definição oficial descreve o World Wide Web como uma iniciativa de busca de informação hipermídia a longa distância que visa dar acesso a um vasto universo de documentos.

O projeto foi desenvolvido a partir de uma proposta de Tim Berners-Lee, pesquisador do CERN em Genebra na Suiça, de um protocolo que trouxesse para a Internet o uso do hipertexto e da hipermídia [10].

Em Novembro de 1990 o projeto estava concluído. O World Wide Web [11], como foi chamado entrou em funcionamento no CERN em Maio de 1991, sendo então disponibilizado para vários grupos.

A partir daí vários browsers WWW foram desenvolvidos, sendo que o mais importante foi o MOSAIC, que foi criado por Marc Andreessen, do NCSA (National Center for Supercomputing Applications). O MOSAIC trouxe algumas inovações, sendo o primeiro browser que utilizava totalmente os conceitos de hipermídia; era multiplataformas, tendo versões para o UNIX e para o Windows e tinha interface "point-and-click". Todos estes fatores tornaram o MOSAIC responsável pelo início explosivo da Internet .

Por sua vez, Marc Andreessen fundou a Netscape, que teve no seu ponto forte o uso do browser de mesmo nome, o qual era uma evolução do Mosaic.

Basicamente um browser integra as seguintes funções :

- Interface gráfica e "pont-and-click" (uso de mouse);
- Utilização de Hipertexto e Hipermídia;
- Formatação variada de documentos e fontes;
- Suporte para som, imagem, filmes e gráficos;
- Utilização de formulários eletrônicos interativos;
- Utilização de vários protocolos (HTTP, HTTPS, FTP, etc)

A World Wide Web está apoiada no conceito do uso integrado de hipertextos, hipermídia, arquitetura cliente/servidor, com interface gráfica, agradável e estimulante ao usuário, sendo fácil de ser utilizada.

Estes conceitos tornaram a popularidade da Internet cada vez mais crescente. Não é difícil entender o motivo: o hipertexto basicamente é um texto comum, o que equivale a dizer que pode ser lido, armazenado ou editado; porém com conexão (hiperlink) para outros textos, documentos ou mesmo outros endereços (DNS) na Internet.

Hipermídia é um hipertexto que integra outras mídias, como imagens, sons e filmes.

Na arquitetura Cliente/servidor o servidor Web tem como propósito fornecer documentos ao cliente. Este por sua vez faz a interface com o usuário, pedindo documentos especificados pelo usuário e exibindo estes documentos na tela do computador.

1.8 - Crescimento e Popularização da Internet.

O advento da WWW impulsionou o crescimento da Internet. De alguns milhares de usuários, a Internet passou a abrigar milhões de usuários. Após o surgimento do MOSAIC, o crescimento da Internet continuou acelerado e em 1992 o milionésimo host foi conectado à rede. Segundo Paxson [4] *"O tamanho da Internet praticamente dobra a cada ano".*

Os tipos de páginas também passaram a ser diversificadas: Páginas de empresas com informações corporativas ou dados sobre seus produtos, páginas financeiras, páginas com notícias, páginas pessoais com todo tipo de informação que se possa imaginar.

No Brasil a Internet também tem grande disseminação entre várias camadas da população, sendo que a tendência é o número de usuários continuar crescendo. Hoje é possível adquirir computadores preparados para a Internet através de linhas de créditos populares.

Segundo a pesquisa do IBOPE eRatings, realizada em Junho de 2001, existem 11,9 milhões de usuários da Internet no Brasil, contando aqueles que acessam a Web de seu trabalho, escolas, universidades, bibliotecas, etc [12].

Os indicadores do Comitê Gestor da Internet no Brasil [13], apontam que o Brasil é o décimo primeiro país no mundo em hosts conectados à Internet, o terceiro das Américas e o primeiro da América do Sul, em pesquisa realizada em Janeiro de 2001.

Não foi somente o número de usuários que cresceu. Os tipos de páginas destinadas a negócios também. As empresas, que no início viram na Internet uma forma de divulgação de seus produtos, passaram a enxergar a Internet como algo a mais, um verdadeiro ponto de venda.

Por isto, hoje é possível comprar de livros a carros, além de efetuar transações financeiras, como pagar contas, fazer transferência de valores, acessar extratos e uma infinidade de facilidades que nunca se imaginava quando da origem da Internet.

CAPÍTULO 2

O Comércio Eletrônico

Este capítulo mostra diferentes abordagens para o termo “Comércio Eletrônico” e estuda como este termo passou a definir as transações comercias via Internet. Também é estudado como o comércio eletrônico impacta as empresas e as perspectivas de valores e crescimento desta nova forma de fazer negócios.

2.1 – Definição de Comércio Eletrônico.

O termo “Comércio Eletrônico” recebeu diversas definições por pesquisadores das mais diferentes áreas, como Tecnologia, Marketing e Administração.

Comércio Eletrônico tem sido definido de várias formas, mas sempre em torno das idéias de transações, que tem por objetivo final, um negócio; e que utilize uma transação eletrônica como meio.

Segundo Zwass [14], a definição de comércio eletrônico é *“O compartilhamento de informações comerciais, a manutenção de relações comerciais e a condução de transações comerciais através das redes de telecomunicações”*.

No entender de Clarke [15] a definição do termo comércio eletrônico é *“A condução de comércio de mercadorias e serviços com o uso de ferramentas de telecomunicações”*

Kalakota e Whisnton [16] sugerem a existência de três classes distintas de aplicações para o comércio eletrônico: Business-to-business, Business-to-Customer e Within Business, as quais podemos definir da seguinte forma:

2.1.1 – Negócio-a-negócio.

O Business-to-business, mais conhecido como B2B, é o que se pode denominar de interorganizacional.

Uma tradução literal define como: Negócio-a-negócio. E é este mesmo o foco desta modalidade de comércio eletrônico, entre empresas.

No business-to-business, é compreendido como comércio eletrônico o uso de tecnologia da informação para facilitar o relacionamento entre a empresa e seus parceiros comerciais. Entre as principais aplicações interorganizacionais podemos citar:

- Gerenciamento de fornecedor;
- Gerenciamento de estoque;
- Gerenciamento de distribuição;
- Gerenciamento de pagamento.

2.1.2 – Interno ao Negócio.

O Within Business é o que podemos definir como aplicações de comércio eletrônico intraorganizacionais.

Esta definição tem como propósito abordar o uso da tecnologia da informação internamente na organização, de forma a ajudar uma companhia a manter relacionamentos que são críticos para uma entrega de valor superior ao cliente. Isto é possível devido à integração de várias funções numa organização.

Esta modalidade é particularmente importante quando a empresa tem filiais geograficamente distribuídas ou está organizada em “unidades de negócio”. Com a consolidação da globalização, uma empresa pode estar representada em vários países e continentes. Nestes casos a comunicação interna é fator determinante dos resultados que podem ser alcançados.

Nesta perspectiva, o comércio eletrônico facilita as seguintes aplicações de negócios:

- Comunicações de grupo de trabalho;
- Publicação eletrônica;
- Produtividade da força de vendas.

2.1.3 – Negócio-a-cliente.

O Business-to-customer, também conhecido como B2C, é o que podemos denominar como negócio-a-cliente, ou seja, entre a empresa e o consumidor final,

No business-to-customer, o comércio eletrônico é dirigido ao consumidor final que, através do uso da tecnologia da informação e da telecomunicação, pode ter acesso aos produtos disponíveis, conhecê-los melhor (especificações técnicas), comprá-los e até efetuar o pagamento através deste meio.

A introdução do B2C, criou uma nova forma de aproximação entre a empresa vendedora e o consumidor.

Basicamente podemos destacar:

- Na perspectiva do consumidor, o comércio eletrônico facilita as transações econômicas;
- Interação social;
- Gerenciamento de finança pessoal;

- Informações e compra de produtos.

Ainda podem ser definidos como modalidades de comércio eletrônico, os seguintes conceitos, segundo Clarke [15] :

2.1.4 – Negócio - Administração Pública.

Esta modalidade de comércio eletrônico engloba as transações eletrônicas entre empresas e o Estado (órgãos públicos e institutos governamentais), sendo também denominada: B2G / G2B (Business to Government / Government to Business).

Nesta modalidade existe um fornecedor, que é o Estado, e um consumidor que é a empresa.

Podemos citar como transações:

- Pagamento eletrônico de taxas
- Emissão de guias, registros públicos e contratos.
- Declarações de informações das empresas ao Estado.

2.1.5 – Consumidor - Administração Pública.

Este conceito de comércio eletrônico engloba as transações eletrônicas entre as pessoas físicas (cidadãos) e o Estado (órgãos públicos e institutos governamentais).

Esta modalidade possibilita basicamente os mesmos serviços encontrados na categoria Negócio - Administração pública, sendo também denominada: B2C

No caso brasileiro, podemos dar ênfase às declarações de imposto de renda, que, a cada ano que passa, vem apresentando um crescimento na porcentagem de formulários de I.R. entregues via Internet.

Estas duas modalidades são conhecidas também como “Governo Eletrônico”.

No Brasil foi constituído o Comitê Executivo do Governo Eletrônico [17], através do decreto presidencial de 18 de Outubro de 2000 que definiu a criação do governo eletrônico brasileiro (e-Gov).

Como podemos concluir o termo “comércio eletrônico” está sempre ligado à tecnologia da informação e ao uso desta para conduzir negócios. Porém este termo não é novo e as suas várias concepções existem há mais de 20 anos [18].

O comércio eletrônico anterior à Internet é denominado: “Comércio eletrônico tradicional”, e pode ser exemplificado através do EFT e do EDI.

O EFT (Eletronic Funds Transfer) surgiu na década de 70. Utilizado entre bancos, através de redes privadas seguras, trouxe grandes ganhos de produtividade para as instituições financeiras. Os pagamentos tornaram-se eletrônicos, através da transmissão eletrônica da informação.

O EDI (Eletronic Data Interchange) surgiu entre o final da década de 70 e o início da década de 80.

O EDI levou o comércio eletrônico tradicional até as empresas, permitindo que estas trocassem informações comerciais através de mensagens eletrônicas em redes privadas.

Porém o termo comércio eletrônico se tornou mais popular recentemente, devido ao uso da Internet e ao aparecimento da WWW (World Wide Web).

Para enfatizar o uso da Internet como meio para o comércio eletrônico, ou e-commerce, surgiram termos como “Internet business”, “Internet commerce” e “Internet Market” [19].

Se compararmos o comércio eletrônico tradicional com o comércio eletrônico através da Internet, podemos ter o seguinte quadro:

	C. E. Tradicional	**C. E. na Internet**
Modalidades	Empresa a Empresa	Negócio a Negócio (B2B) Cliente a Negócio (B2C) Intraorganizacional Negócio – Administração Pública Consumidor – Administração Pública
Usuários	Específicos a cada setor, parceiros limitados	Mercado aberto, escala global.
Tecnologia	Redes específicas	Redes abertas
Segurança	Segurança na concepção da rede	Há necessidade de implementar mecanismos de segurança.
Mercado	Mercado fechado	A rede é o mercado

Tabela 2.1 : Comércio eletrônico tradicional x Comércio eletrônico na Internet.

De uma forma genérica, atualmente, o termo “comércio eletrônico” designa o uso da Internet (Web) para compra e venda de produtos, bem como a divulgação e o acesso a estes produtos, por parte do consumidor final (B2C).

Também serve para definir o uso da Internet entre as empresas, desde que existam objetivos comercias nesse relacionamento (B2B).

Assim, podemos concluir que o termo “comércio eletrônico” envolve o compartilhamento de informações comercias através da Internet, o uso da Internet para se manter relações comerciais e a condução de negócios através do uso da Internet.

2.2 – O Comércio Eletrônico do ponto de vista financeiro.

Segundo Kotler [20], o marketing se baseia em produto, ou seja, efetivamente o que se está tentando vender; em propaganda, que é todo esforço feito para a aceitação do produto junto ao público; em preço, isto é, um preço competitivo; e em ponto de venda, que é onde o produto é oferecido ao público.

Segundo Santos [21] *"O comércio eletrônico possibilita enfocar a Internet como um canal de distribuição de produtos*".

Podemos então considerar a Internet como um verdadeiro ponto de venda para as empresas que lançam mão do uso do comércio eletrônico da Web, principalmente quando enfocamos o B2C.

É comum para qualquer usuário da Internet ao entrar em um site de algum grande banco, ou em algum portal de notícias, ter a sua disposição uma série de ofertas, das mais diversas formas de produtos a venda no próprio site, ou em um link de uma página específica para o comércio eletrônico.

O comércio eletrônico vem sendo considerado, até de forma exagerada, uma verdadeira revolução para as empresas. Assim como nas décadas de 70 e 80 os shopping centers se tornaram um ponto de referência dos centros urbanos no mundo moderno, o comércio eletrônico veio para mudar a forma das empresas e do público de modo geral.

Segundo Jerry Yang da Yahoo!: *"Na essência, o comércio eletrônico não é apenas a criação de novos negócios, mas também o nascimento de uma nova cultura de conveniência e rapidez"* [22].

Para centenas de empresas no varejo, essa realidade chegou de forma cruel. A Enciclopédia Britânica, entidade com 230 anos de tradição, teve que dispensar

todos os vendedores que tinha no território norte-americano, por que o mesmo conteúdo que a enciclopédia continha, pode ser pesquisado através da Internet de forma gratuita, enquanto os 32 volumes da enciclopédia custavam em média 1.250 dólares, tornando inviável sua venda.

Desintermediação é o novo termo usado para ilustrar o caso acima citado. Significa a eliminação dos intermediários, despachantes de operações de qualquer economia, tais como agentes de viagem, corretores de Bolsas de Valores, vendedores de carros e vendedores ambulantes.

2.3 – Movimentação Financeira.

Segundo o Edge Research Group, empresa de consultoria especializada em produzir números sobre a Internet, as empresas que se dedicam a vendas utilizando-se do comércio eletrônico no Brasil estarão movimentando aproximadamente 4 bilhões de dólares até o ano de 2003 [23].

Segundo a pesquisa ainda, a estimativa é que de tudo que será vendido no Brasil no ano de 2002, 24% das vendas serão eletrônicas.

A pesquisa anterior do mesmo grupo, realizada 2 anos antes, indicava que em 2002 seria de 12% a fatia das vendas eletrônicas, o que demonstra que o crescimento tem se mostrado acima do esperado.

Apesar do desaquecimento do comércio varejista tradicional, devido à instabilidade financeira do Brasil no ano de 2002, uma pesquisa fomentada pela FEA (Faculdade de Economia, Administração e Contabilidade da USP) mostrou que o comércio eletrônico brasileiro continua crescendo [24].

As expectativas em relação ao comércio eletrônico brasileiro são muito boas, ainda mais, se considerados os índices da Fundação Getúlio Vargas, que apontam para uma baixa participação de empresas brasileiras no comércio eletrônico: 1,18% nas transações B2B e 0,35% nas transações B2C [25]. Vale deixar claro que mesmo assim, o Brasil ainda é o líder em negócios eletrônicos na América Latina.

Porém, apesar de todas expectativas positivas para o comércio eletrônico, as empresas que disponibilizam um site na Internet, devem ter seus objetivos bem claros. Segundo Bruner [26]: *"A web pode ser uma ramificação altamente econômica de um programa de marketing geral de uma empresa, mas ela também pode significar um rombo financeiro colossal se a empresa não determinar os objetivos específicos para utilizá-la"*.

CAPÍTULO 3

Segurança na Internet e o Comércio Eletrônico

Este capítulo mostra que a Internet não é um ambiente totalmente seguro. Nem todos seus usuários estão imbuídos de boas intenções. Esta insegurança anárquica pode acabar refletindo em uma desconfiança por parte dos usuários no uso de aplicações de comércio eletrônico.

3.1 – Insegurança na Internet.

Como pudemos notar no primeiro capítulo, a Internet não nasceu de forma planejada, não tinha o objetivo de atingir tantas pessoas, em tantos locais distintos do planeta.

O objetivo inicial, ainda na ARPANET, era apenas assegurar que a comunicação de dados pudesse ser mantida em uma situação extrema. Nem de longe se sonhava que além de atingir o número de pessoas que hoje faz parte da Internet, pudesse conter tão diferentes objetivos.

A rede foi projetada com a finalidade de atender as Forças Armadas Americanas. Como conseqüência, apesar de existir uma grande preocupação com a robustez da rede, que deveria continuar funcionando mesmo após um possível ataque nuclear, não existia preocupação com a segurança das informações que trafegariam na rede.

Desta forma, quando se faz uma reconstituição do surgimento da Internet, não é encontrada nenhuma referência sobre criptografia dos dados, ou qualquer outro método de encapsulamento das informações transmitidas, que tivesse por objetivo manter a inviolabilidade das mesmas.

Infelizmente a Internet não é um ambiente onde somente existem pessoas com intuito de utilizá-la em benefício próprio ou de outros. Existem pessoas cuja intenção é danificar dados ou equipamentos, interferir em comunicações ou até mesmo roubar dados ou valores de outras pessoas.

Existe uma série de termos [27] para definir estas pessoas que utilizam a Internet para, através do seu computador, realizar ataques a outros computadores: Hacker, Cracker, Script Kid, Phreaker, Wannabe, Lamer, etc.

Destes vale a pena destacar:

- **Hacker** - O termo hacker, designa qualquer pessoa extremamente especializada em uma determinada área. Porém, a sua utilização mais comum é para definir pessoas que possuem uma grande facilidade de análise, assimilação, compreensão e facilidade de manuseio de um computador. O hacker utiliza estas habilidades para invadir um computador na rede através de falhas existentes no sistema de segurança, porém, sem corromper informações ou danificar sistemas. Normalmente o próprio hacker escreve os programas que utiliza para realizar a invasão.

- **Cracker** - É o hacker que utiliza suas habilidades com o computador para realizar ataques mal intencionados. O cracker utiliza seus conhecimentos

para danificar dados, obter senhas de sistemas, acessar informações sigilosas, e até mesmo, se apossar de valores de terceiros, cometendo o que é definido como crime cibernético.

- **Script Kid** – É um termo pejorativo, que os hacker utilizam para definir o aspirante a hacker ou cracker. O script kid se julga um hacker, mas não tem o conhecimento técnico que um hacker tem. Ele apenas se utiliza de ferramentas desenvolvidas por hackers para realizar ataques e invasões em sistemas. O script kid sabe utilizar o programa de invasão, porém não tem conhecimento suficiente para compreender o funcionamento do mesmo.

Apesar de toda esta gama de termos, para grande parte dos especialistas em segurança de redes e do público em geral, o termo hacker está consagrado como sinônimo de invasor de sistemas [28].

Desta forma nesta dissertação, será utilizado apenas o termo hacker, sem fazer nenhuma distinção, entre hacker, cracker, script kid, ou qualquer outro termo que possa ser associado ao usuário invasor de máquinas da rede.

Normalmente, o hacker sabe que pode encontrar alguma falha no sistema de segurança e sabe como procurar por elas. Utilizando de várias técnicas, contando com força de vontade e tempo disponível para viabilizar suas idéias, ele pode conseguir algumas proezas, deixando muitas vezes uma imagem de insegurança e de total falta de privacidade na Internet.

Para ilustrar, podemos citar a seguinte notícia, que foi destaque nos principais meios jornalísticos, inclusive na própria Internet, veiculada em Março de 2001:

Um jovem britânico, Raphael Gray, então com 19 anos, invadiu um site de e-commerce e conseguiu acessar dados bancários de 23.000 pessoas, publicando-os na Internet.

Não bastasse isto, para provar que os dados eram verdadeiros e que o ambiente invadido era inseguro, Gray comprou via Internet, um medicamento popular enviando-o ao próprio dono do cartão de crédito, que foi utilizado para pagar a compra. Para reforçar ainda mais a imagem de insegurança na Internet, a vítima escolhida por Gray, era o presidente da Microsoft, Bill Gates.

Ao ser entrevistado, Gray deu a seguinte declaração:

"Sou a favor do comércio on-line, desde que seja seguro e razoável: algo que é raro nos nossos dias. Queria mostrar como estes sites são inseguros, por isso publiquei a informação na Internet. Não tinha escolha, se eu entrei no sistema, qualquer um poderia ter invadido também" [29].

Fatos como estes não acontecem todos os dias, porém, notícias sobre invasões, novos vírus, falhas de segurança em sistemas operacionais e outras notícias do gênero, podem ser observados diariamente, em sites nacionais ou internacionais, dedicados a segurança de informações, ou em publicações especializadas em informática. Entre estes sites podemos citar o www.securenet.com.br e o www.cert.org.

3.2 – Insegurança X Comércio Eletrônico.

Pelo que se conclui do capítulo anterior, o comércio eletrônico é um negócio altamente promissor, onde muita gente tem investido e podemos concluir que os

volumes envolvidos são altíssimos. Por isso mesmo, o fator segurança deve ser um item altamente preocupante para quem pretende investir no comércio virtual.

Afinal é necessário garantir que os bilhões de dólares que trafegam na rede, além das informações sigilosas das empresas envolvidas e de seus clientes, estejam a salvo de usuários mal intencionados.

Só para se ter uma idéia, uma única empresa, o Banco do Brasil, movimentou R$ 8,8 bilhões através da Internet no ano de 2001, segundo a pesquisa Info 100, da revista Info Exame, que classificou as 100 empresas que mais movimentaram valores através da Internet, em 2001 no Brasil [30].

Segundo Zaninotti [31]*, "Além de lidarmos com adolescentes com objetivo claro de chamar a atenção das pessoas, existem criminosos com objetivo de prejudicar a imagem de empresas e principalmente, obter acesso a informações privadas"*.

Afinal, além dos valores envolvidos, existe outro motivo que pode atrair a atenção de quem queira aplicar um golpe cibernético. Segundo Jim Wygand presidente da Control Risk do Brasil, empresa especializada em investigação de crimes cometidos em empresas, *"Os crimes eletrônicos são muito menos arriscados e mais lucrativos*" [32].

Normalmente os crimes que envolvem a Internet são relativos a golpistas que, de alguma forma, conseguem ter acesso aos dados de clientes: Número de conta corrente, senha, ou dados do cartão eletrônico. De posse destas informações, conseguem efetuar saques ou realizar transferências de valores.

Estes crimes podem ser perpetrados através da Internet ou do uso de caixas eletrônicos; porém estes dados são conseguidos de forma comum, ou seja, pessoas que não são cuidadosas com suas senhas e cartões; e que de alguma forma se

deixam enganar por estelionatários que, de posse destas informações, passam a fazer movimentações nas contas ou cartões de crédito, das vítimas.

Segundo o especialista em segurança Steven Bellovin, Phd em Ciência da Computação e consultor do governo Norte-americano para assuntos de segurança de redes: *"Hackers não são especialistas em criptografia, mas sim trapaceiros*" [33].

Apesar de não existir notificação de casos de quebra de criptografia, os casos envolvendo roubo de senha, crimes que envolvem uso de cartões eletrônicos, a divulgação constante por parte da mídia da ação de hackers por todo o mundo e a constante proliferação de vírus enviados através do correio eletrônico, trazem ao usuário da Internet uma sensação de insegurança que permeia um grande número de usuários, afastando-os da Internet, ou pelo menos, afastando-os das aplicações comerciais ou financeiras.

Desta maneira, implementar ferramentas que tornem o uso de transações na Internet seguras, além de proteger o patrimônio próprio e o patrimônio dos clientes, é também uma forma de manter e conquistar novos clientes.

É comum a qualquer pessoa que utiliza com certa freqüência o computador e tenha o mínimo conhecimento sobre o funcionamento do mesmo, que se sinta insegura ao utilizar a Internet em transações que envolvam dados sigilosos.

Segundo uma pesquisa realizada em 1998 pela Yankelovich Partners [34], 85% dos usuários de Internet se sentem incomodados ao enviar números de cartão de crédito pela Internet, devido a possível falta de segurança da mesma.

Não é só o usuário comum que pode se sentir ameaçado. Segundo o instituto de pesquisas Datamonitor os prejuízos decorrentes de invasões eletrônicas em todo o mundo chegaram a 15 bilhões de dólares no ano 2000 [35].

No Brasil, o ISS (Internet Security Systems) fez uma pesquisa entre as 200 maiores empresas brasileiras, que apontou que 70% destas empresas registraram alguma forma de ataque aos seus sites corporativos [36].

O fator segurança na Internet tem sido uma grande preocupação para o estabelecimento de uma aceitação maior para a utilização de aplicações comerciais na Web.

O assunto segurança da informação é objeto inclusive da norma internacional ISO 17799, que foi baseada na BS 7799 produzida pelo BSI (British Standard Institute) e que no Brasil foi adotada pela ABNT (Associação Brasileira de Normas Técnicas), com o código NBR ISO/IEC 17799 [37].

Para a implementação de transações tais como Home Banking, compras por cartão de crédito, ou qualquer outra informação que se deseja proteger, os usuários de parte a parte desejam assegurar-se de que as transações sejam completamente confidenciais e isentas de alterações indevidas feitas por terceiros.

Mecanismos de segurança têm sido desenvolvidos para implementar a confiança necessária às aplicações de comércio eletrônico, introduzindo confidencialidade nas transações por meio de algoritmos de criptografia dos dados transmitidos, autenticação eletrônica, segurança de integridade das mensagens e da identificação de origem.

Estes mecanismos podem, conjuntamente, desde que bem implementados, garantir o sucesso das transações eletrônicas, afastando os hackers do conteúdo das informações que se deseja proteger e serão objeto de estudo nos próximos capítulos desta dissertação.

3.3 – Observando a realidade.

Desde que o comércio eletrônico, ganhou um novo impulso, com o advento da Internet, o tema “Segurança na Internet” tem sido amplamente discutido.

É muito fácil encontrar este assunto sendo abordado em diversos sites, revistas, livros específicos e até mesmo em programas populares de rádio, que contam com a participação de especialistas em informática, a fim de dirimir dúvidas de seus ouvintes.

Porém, as ações das empresas no que se refere a segurança, ainda são controversas e muitas vezes, ainda deixam a desejar, dado todas as possibilidades de riscos envolvidos.

Como base, podemos tomar a última pesquisa divulgada pela Módulo Security Solutions S.A., sobre Segurança da Informação, divulgada em Julho de 2001 e realizada com executivos das grandes empresas brasileiras [36] :

- 94% dos entrevistados reconhecem a grande importância da proteção de dados.
- 56% consideram a proteção de dados vital para a corporação.
- 63% acreditam que os problemas com a segurança tendem a crescer.

Estes dados reforçam a idéia de que a segurança dos dados deve ser alvo de grande interesse das empresas, principalmente aquelas que se utilizam da Internet. Porém, na mesma pesquisa, podemos encontrar as seguintes informações:

- 46% dos entrevistados não possuem nenhum plano de ação em caso de ataques.
- 40% das empresas já sofreram algum tipo de invasão .

- 31% não tem condições de precisar se sofreram ou não algum ataque.
- 57% das empresas que sofreram ataques, apontam a Internet como o principal ponto de invasão.

Ou seja, as empresas reconhecem a importância da segurança de dados, porém muitas não estão preparadas para reagir caso venham a sofrer um ataque.

Muitas já sofreram ataques e apontaram que o principal foco de invasão é a Internet, e 36% dos entrevistados acreditam que os hackers possam representar alguma ameaça a suas empresas.

A grande maioria, 53%, aponta possíveis funcionários insatisfeitos como a maior ameaça às informações, e as invasões internas representam 23% dos ataques acontecidos.

O que se pode concluir é que, se muito já foi feito pela segurança das transações eletrônicas, muito ainda há por se fazer para que o comércio eletrônico possa ser totalmente seguro e livre de riscos para ambas as partes.

Para que se possa chegar ao nível desejado de segurança de dados, se faz necessário conhecer:

- Os requisitos básicos de segurança;
- Os riscos existentes, que colocam em xeque estes requisitos mínimos e os principais ataques conhecidos, que permitem perpetrar esta situação de risco;
- Os mecanismos de segurança, que existem para implementar estes requisitos básicos e eliminar os riscos existentes.
- As principais ferramentas desenvolvidas que permitem a implementação destes mecanismos.

Cada um destes itens é importante. Os responsáveis pela segurança dos dados de cada empresa e os usuários devem estar cientes desta importância.

Desta forma, esta dissertação vai dedicar um capítulo para o estudo de cada um destes itens, a fim de explicitar todos estes conceitos envolvidos.

CAPÍTULO 4

Garantias necessárias ao Comércio Eletrônico.

Este capítulo mostra, as principais garantias de segurança que devem existir para o sucesso das transações de comércio eletrônico através da Internet.

A importância desde capítulo é justificada pelo fato de que não se pode analisar os riscos existentes se não soubermos primeiro o que se quer proteger e o que se deseja garantir.

4.1 – Privacidade.

De uma forma geral, toda questão que envolve a segurança de dados, seja no tráfego das informações ou no armazenamento de dados, está relacionada a garantia de privacidade que se deseja obter.

Através de Clarke [38], obtemos a seguinte definição: *"Privacidade é o interesse que cada indivíduo tem de manter um 'espaço pessoal', livre da interferência de outras pessoas ou organizações"* .

Ainda sobre os critérios do autor citado, podemos encontrar o termo privacidade sobre quatro dimensões distintas:

- Privacidade pessoal;
- Privacidade do comportamento pessoal;
- Privacidade das comunicações.
- Privacidade dos dados pessoais.

Entre estas devemos destacar:

4.1.1 - Privacidade das comunicações.

É o fato das pessoas trocarem informações por vários meios, como por exemplo: Correio, telefone, rede de computadores, etc; sem que exista um monitoramento destas comunicações.

Para que isto seja garantido, não pode haver interceptação destas comunicações.

4.1.2 – Privacidade dos dados pessoais.

Ao efetuar negócios, as pessoas declaram informações pessoais que ficam em poder de terceiros.

Como exemplo pode-se tomar: Cadastros, fichas de propostas, comprovantes de cartão de crédito e qualquer outra forma onde dados de pessoais ficam armazenados.

A garantia que estas informações não serão acessadas por pessoas não autorizadas, está relacionada à privacidade dos dados pessoais e privacidade das informações.

Genericamente se pode utilizar o termo “Privacidade da Informação”, para determinar o interesse que as pessoas têm em controlar seus dados pessoais.

Esta definição pode ser aplicada à Internet, uma vez que os conceitos de privacidade das comunicações e privacidade dos dados pessoais, são objetivos que se quer atingir em segurança de redes.

No entanto, para especialistas em segurança de redes, cientistas da computação e especialistas em informática, os termos mais comuns, utilizados para

designar a privacidade das informações em meios computacionais, seja no armazenamento, ou na transmissão dos dados, são : Segurança dos dados e segurança na transmissão dos dados.

4.2 – Confidencialidade.

As empresas para poderem atuar em algum segmento do mercado, têm que ter conhecimento sobre esta sua área de atuação. Este conhecimento adquirido sobre o negócio envolve: a forma de conduzi-lo, os clientes, informações sobre o processo produtivo, aspectos financeiros da organização, entre outros.

É comum que as empresas tentem resguardar estas informações de pessoas não autorizadas, a fim que estas informações não sejam utilizadas por empresas concorrentes.

Manter em segredo estas informações significa que elas são sigilosas, que se quer, portanto, garantir o sigilo ou a sua confidencialidade.

Da mesma forma, este raciocínio é mantido quando o termo confidencialidade é empregado na Internet, ou em segurança de redes de um modo geral.

Nesse caso, garantir o sigilo, ou garantir a confidencialidade das transações eletrônicas significa dizer que os dados que trafegam na rede não podem ser observados por terceiros.

Assim sendo, para garantir o sigilo, dois requisitos básicos devem ser atendidos durante a transmissão eletrônica dos dados [39]:

- Ninguém pode observar o conteúdo da mensagem eletrônica

- Ninguém pode identificar quem está enviando e quem está recebendo a mensagem eletrônica

Isto significa que, em uma transação de comércio eletrônico, deve-se garantir que o conteúdo da transação (valores, prazos, etc) e as partes envolvidas (comprador e vendedor), não podem ser identificados por algum intruso que esteja tentando monitorar o que está trafegando na rede.

4.3 – Integridade.

No mundo dos negócios convencionais, toda empresa quer garantir que as informações existentes na entrega de uma encomenda em seu destino sejam exatamente iguais as informações que foram criadas quando da geração do pedido da encomenda citada.

Desta forma, pode-se definir integridade como a manutenção da informação tal qual ela foi gerada. Isto é, garantir que o conteúdo da informação inicial, seja fielmente reproduzido na informação final.

O conceito de integridade para o comércio eletrônico, ou de maneira geral, para todo o ambiente de segurança de redes é semelhante, porém mais complexo.

Segundo Clarke [39], para garantir a integridade ou o conteúdo da mensagem, é necessário atender as seguintes condições:

- A informação não pode ser modificada ou perdida durante a transmissão.
- A informação não pode ser prevista antes de chegar ao seu destino.
- A informação gerada não pode ser modificada na origem, nem mesmo no destino por pessoas não autorizadas.

Para isto, é preciso ter mecanismos que impeçam que a mensagem seja interceptada e alterada durante sua transmissão, bem como, dispor de mecanismos que impeçam que a informação possa ser acessada, por pessoas não autorizadas, nos computadores onde a informação estiver armazenada.

4.4 – Autenticação.

A autenticação é o mecanismo através do qual se quer garantir que as entidades que estão negociando são realmente quem dizem ser.

Com a autenticação se quer garantir que os envolvidos sejam válidos e afastar a possibilidade de um impostor perpetrar ações fraudulentas.

Desta forma, no mundo dos negócios convencionais é muito comum as seguintes situações:

- Vendedor, para aprovar uma ficha de crédito, solicita comprovantes de residência e renda, junto ao comprador (Exemplos: Contas, contratos, comprovantes de pagamentos, etc).
- Vendedor, ao receber o pagamento em cheque, ou cartão de crédito, solicita documentos que comprovem a identidade do comprador (Exemplos: Carteira de identidade, carteira de trabalho, etc).
- Comprador ao receber um vendedor em sua casa, solicita documento que comprove que o vendedor pertence à empresa que representa (Exemplos: Carteira funcional, contrato, etc).

- Em um atendimento bancário telefônico, a atendente confirma dados pessoais, para garantir que quem está sendo atendido é realmente quem diz ser (Exemplos: Data de nascimento, endereço, etc).

Da mesma forma, no comércio eletrônico é necessário que exista a autenticação.

Neste caso, porém, sempre se deseja determinar que as entidades envolvidas na transmissão de dados sejam quem realmente dizem ser.

Num exemplo prático podemos dizer que, numa operação de Internet Banking, o cliente tem que ter certeza que está enviando seus dados (conta, senha, valores, etc) para a instituição bancária desejada. Assim como o banco tem que ter certeza que quem está enviando as informações é um cliente autorizado.

Assim podemos resumir desta forma [39]:

- Quem gera a informação deve estar certo que a informação chegará ao destinatário desejado.
- Que a informação gerada chegará somente ao destino desejado.
- O destinatário, que recebe a informação, deve estar certo que esta informação veio do emissor original, não de um impostor.

4.5 – Não repúdio.

Para se entender o que é o não repúdio é necessário primeiro definir o que é o repúdio.

Repúdio é o fato de se negar a participação numa determinada operação. O problema realmente surge se a negativa, ou seja, o repúdio, acontecer sobre uma operação que de fato ocorreu.

O não repúdio é o termo utilizado para designar a qualidade de uma transação que não pode ser negada.

No comércio convencional, a forma mais comum de garantir o não repúdio é através da assinatura das partes envolvidas, que pode ter a participação de testemunhas, ou de um documento que não seja possível negar a emissão.

Nestes casos, até um perito grafotécnico pode opinar sobre a veracidade de alguma assinatura sobre a qual se tenta repudiar a origem.

Como exemplo podemos citar:

- Ao receber um pagamento em cheque, o vendedor confronta a assinatura do cheque com a assinatura de algum documento.
- Ao receber o pagamento com cartão de crédito, mesmo que o cartão esteja liberado através de uma consulta própria, o vendedor requisita a assinatura do comprador.
- O comprador exige a nota fiscal para comprovar a compra da mercadoria.

Nas transações eletrônicas também deve existir o conceito de não repúdio, aliás, de uma forma até mais completa, pois o conceito deverá ser sempre bidirecional.

Assim sendo [39]:

- Quem gera a transação eletrônica não pode negar que o envio da mesma foi realizado por ele.

- Quem recebe a transação eletrônica não pode negar o fato de tê-la recebido.

4.6 – Autorização.

A autorização é um complemento da autenticação. Enquanto no procedimento de autenticação se quer garantir que as pessoas que estão transacionando são de fato quem dizem ser, no procedimento de autorização se quer determinar que esta pessoa devidamente autenticada, tenha autorização para efetuar a transação que está realizando.

Em transações convencionais, pode-se exemplificar:

- Determinação de limites de valores para autorização de pagamentos.
- Exigência de mais de uma assinatura em cheque para autorizar o pagamento.

A autorização está intimamente ligada ao controle e limitação de acesso e assim como nas transações convencionais, deve também existir no comércio eletrônico.

Em ambientes computacionais a autorização está normalmente sendo implementada através da atribuição de níveis de permissão ao usuário envolvido, através de seu nome de usuário e respectiva senha de acesso.

4.7 – Registro.

Em qualquer atividade comercial convencional, a transação efetuada deve ser devidamente registrada. O registro da transação é a prova que ela de fato ocorreu.

No ambiente de qualquer empresa é normal que existam:

- Emissão de nota fiscal, ou cupom que tenha validade fiscal.
- Registros de entrada de mercadorias.
- Registros de saída de produtos.
- Lançamentos contábeis.

Estes exemplos, entre outros, são formas de se registrar que houve uma operação comercial e que esta de fato possa ser comprovada através destes registros.

No comércio eletrônico o registro das transações deve existir da mesma forma, ou seja, uma determinada operação realizada por um usuário remoto, deve ser recuperável, para que se possa comprovar a veracidade da mesma.

Assim sendo:

- Quem recebe a transação eletrônica deve armazená-la.
- Quem gera a transação deve armazenar cópia da mensagem enviada.
- Em ambos os casos esta transação deve ser armazenada em meio seguro e deve existir garantia de que a mesma possa ser recuperada.

CAPÍTULO 5

Principais riscos à segurança dos dados na Internet

Este capítulo mostra os principais riscos e formas de ataque existentes à segurança dos dados de um computador que esteja conectado a Internet. A importância desde capítulo é justificada, uma vez que não podemos analisar corretamente as ferramentas e mecanismos de defesa existentes se não conhecermos primeiro os riscos e ataques existentes.

De uma forma mais abrangente, podemos dizer que todos os problemas estudados neste capítulo estão, de certa forma, relacionados à quebra da privacidade do usuário na Internet e nas redes de um modo geral.

5.1. – Etapas da transação eletrônica.

A forma mais correta de entender a importância da segurança para o comércio eletrônico é estar ciente dos vários tipos de ameaça à privacidade da informação e buscar as ferramentas corretas para conter estas ameaças.

Para que se possa estudar melhor estas possibilidades, deve-se fragmentar os possíveis pontos de ataque, de acordo com a etapa que representa no processo da transação eletrônica.

Assim sendo, pode-se dizer que a transação eletrônica corre algum risco nas seguintes etapas [40]:

5.1.1 – Antes de ser introduzida no computador.

Esta etapa é representada pela informação que ainda não foi introduzida no computador. A fonte de risco mais presente neste momento é a pessoa que tem acesso aos dados que serão introduzidos no computador. Geralmente, um funcionário mal intencionado, que pode roubar ou modificar estas informações com a finalidade de tirar proveito próprio, ou tão somente prejudicar as pessoas envolvidas na transação.

5.1.2 – No computador de origem.

O computador onde a informação está sendo gerada pode, de alguma forma, ser monitorado, através de um agente invasor, e as informações nele contidas, serem manipuladas ou roubadas, por este mesmo agente.

5.1.3 – No transporte da informação entre a origem e o destino.

Através de dispositivos de hardware ou software, algum agente externo pode ter acesso às informações que trafegam na rede, obtendo dados sigilosos, apenas com o intuito de observar informações não autorizadas, ou até mesmo alterando o conteúdo destas informações, danificando a transação eletrônica.

5.1.4 – No computador destino.

Assim como no computador de origem, o computador destino pode ser invadido através de alguma forma de ataque.

Se o sistema de segurança de dados do computador onde os dados referentes à transação eletrônica estiverem armazenados não for eficiente, estes

dados podem ser violados e as informações pessoais e comerciais, contidas no computador destino, cair em posse de intrusos.

5.2 – Ações fraudulentas.

Cada uma destas etapas, conforme exposto, possibilita que a transação eletrônica corra um determinado risco, estando sujeita a diferentes tipos de fraudes, que podemos basicamente dividir da seguinte forma:

5.2.1 – Interceptação da transmissão.

A interceptação de dados ocorre quando alguém, através de recursos de hardware ou de software, consegue espiar os dados que trafegam na Internet, ou em ambientes de rede de um modo geral.

Desta forma, dois dos conceitos estudados no capítulo anterior, que devem existir para garantir transações de comércio eletrônico, estarão comprometidos: A confidencialidade e integridade das informações.

Se houver interceptação destes dados, haverá um grande risco que informações sigilosas, como por exemplo: dados pessoais, número de cartão de crédito, número de conta corrente e sua respectiva senha, entre outras informações; possam ser utilizadas pelo hacker que se apossou das mesmas.

Caso estes dados estejam encapsulados por algum processo criptográfico (mecanismo que será discutido no capítulo 6), mesmo que o hacker os tenha armazenado em seu próprio computador, dificilmente conseguirá decifrar e fazer uso das informações que acessou.

Para que o segundo conceito seja atingido, a integridade das informações, os dados interceptados pelo intruso, devem ser alterados.

Esta alteração pode ter várias motivações, desde alguém que apenas queira atrapalhar a comunicação, gerando uma informação inválida; como alguém que queira fazer estas alterações em beneficio próprio, como por exemplo: uma compra ser entregue em um endereço, diferente do determinado e que interesse ao hacker invasor; ou ainda, parte do saldo de uma conta corrente ser desviado para uma conta que o hacker possa manipular.

5.2.2 – Falsificação de identidade.

É a situação onde o hacker assume a identidade de outro usuário. Isto se dá no momento em que uma pessoa assume uma identidade falsa perante um outro usuário da rede.

Este tipo de fraude pode ser realizado por diferentes motivos, desde alguém que deseje esconder sua verdadeira identidade como, num caso mais extremo, alguém que deseje prejudicar diretamente o verdadeiro dono da identidade assumida.

Para que a falsificação seja efetuada, dois dos conceitos estudados deverão ser comprometidos, a Autenticação e a Autorização.

No primeiro caso, a pessoa que falsifica a identidade somente será aceita pelo outro envolvido na transação caso o conceito de autenticação não seja utilizado, ou caso o falsificador consiga iludir o sistema de segurança, sendo erroneamente autenticado pelo sistema.

No segundo caso, pode estar o verdadeiro motivo do que se deseja com a falsificação, ou seja, o hacker se passa por outro usuário, para justamente obter as

autorizações que este usuário detém e assim poder realizar transações que somente o usuário autorizado poderia fazer.

5.2.3 – Imitação.

A imitação pode ser definida como o tipo de fraude, onde o hacker consegue se colocar no meio de uma comunicação entre outros dois usuários.

Desta forma, o hacker intercepta e se coloca no meio da comunicação entre dois usuários e de forma minuciosa, consegue controlar esta comunicação.

O controle deve ser realizado de tal forma que um usuário terá a ilusão que está tratando com o outro, mas na verdade ambos estão se comunicando com o hacker, que de forma hábil, repassa as transações, sem que os usuários percebam, podendo modificar as informações de acordo com seu desejo.

Neste tipo de fraude, todos os conceitos de segurança são quebrados.

5.2.4 – Acesso indevido a dados.

O acesso indevido consiste no ato de alguém se apossar de dados não autorizados, obtendo assim, informações que normalmente não poderia dispor.

Esta forma de fraude pode ser perpetrada de várias formas, desde as já vistas anteriormente, como interceptação, falsificação e imitação, bem como formas mais simples, como um funcionário de uma determinada empresa, acessar dados que lhe são proibidos pelas regras da empresa.

O acesso indevido é uma das principais fontes de problemas que as empresas tem na atualidade.

Uma grande parte da quebra de privacidade é advinda de pessoas que normalmente deveriam zelar pela segurança das informações, e de forma contrária, acabam expondo sua fragilidade.

Estes problemas são tão comuns que atingem até mesmo empresas especializadas em segurança de dados.

5.2.5 – Repúdio.

O repúdio é a ameaça que se contrapõe ao que foi visto no item 4.5, o não repúdio.

O repúdio existe no momento em que alguém nega uma transação realizada. O problema, na verdade, pode tomar grandes proporções, quando se nega uma transação que realmente aconteceu [41].

Não é difícil imaginar uma situação em que o repúdio possa ocorrer: Uma pessoa efetua a compra através de alguma aplicação de comércio eletrônico, usando como forma de pagamento o cartão de crédito. A pessoa digita o número do seu cartão e efetua a compra. Porém, quando a fatura da empresa de cartão de crédito é recebida para o pagamento real, o golpista liga para a administradora do cartão, refutando tal compra.

5.2.6 – Repetição de transação.

A repetição consiste na fraude de se repetir uma transação que já ocorreu. Para isto, são necessárias três situações:

- Uma transação de fato efetuada, que seja armazenada por alguém que intercepta esta transação.

- Aquele que interceptou e armazenou a transação, transmiti-la posteriormente.
- O sistema que aceitou estas transações, não dispor de nenhum mecanismo que consiga diferenciá-las

Desta forma, a transação armazenada e repetida pode ser aceita como válida, criando transtornos para o usuário que realizou a transação original e para a empresa que aceitou as transações.

5.3 – Principais formas de ataques.

As diversas formas de ações fraudulentas podem ser perpetradas, através de variadas técnicas, que são denominadas genericamente de “ataques”.

Estes ataques, normalmente são conhecidos. Porém, mesmo assim continuam oferecendo perigo para usuários desprotegidos.

Entre estes ataques, alguns são clássicos e serão destacados nesta dissertação.

5.3.1 – Social Engineering (Engenharia Social).

O termo “Engenharia Social” é utilizado para designar um conjunto de técnicas de burla, utilizadas por estelionatários para se apossarem de informações que deveriam ser restritas a seus proprietários.

Na verdade, a engenharia social é apenas uma adaptação de técnicas de estelionato ao ambiente informatizado e à transferência eletrônica de dados [42].

Estas técnicas de criminalidade existem de longa data, sendo popularmente conhecidas como “O conto do vigário”.

Existem casos de estelionatários que se passam por operadores de telemarketing de um banco qualquer, e ligam para um determinado cliente, envolvendo a vítima de tal forma que conseguem a conta, a senha e demais dados sigilosos da mesma.

5.3.2 – Sniffer.

O sniffer é um ataque que viabiliza a interceptação de dados. Esta técnica presume que um computador em uma rede esteja em modo promíscuo. Isto é, este computador observa e recupera informações que passam pela rede e que não estejam endereçadas a ele [43].

Este tipo de ataque está associado ao uso de uma LAN (Local Area Network), pois normalmente os pacotes que são destinados a uma determinada máquina da rede circula por toda a rede, porém, somente é acessada pela máquina de destino.

Se um computador é manipulado para ficar em “Promiscuous Mode”, todas as informações que passam por este computador podem ser acessadas e armazenadas por esta máquina, mesmo os pacotes de dados que não foram endereçados a ele.

Se o hacker que introduziu este programa no computador souber decifrar estas informações, ele poderá acessar dados como senhas, nomes de usuários e outras informações sigilosas.

Apesar deste tipo de ataque estar associado ao ambiente de uma LAN, isto não significa que não possa ser perpetrado através da Internet. É comum que

empresas que possuam redes locais estejam também ligadas à Internet, de forma que as máquinas da rede possam acessar a Internet.

Uma das máquinas pertencente à rede pode ser invadida por um hacker e este pode instalar um sniffer com recurso de log file. Isto é, um arquivo que vai armazenar dados referentes a acessos (nomes e senhas) que trafegarem pela rede.

Desta maneira o hacker pode voltar a entrar na máquina invadida e recuperar este arquivo, dispondo assim de informações que deveriam pertencer somente aos seus responsáveis.

5.3.3 – Dos ou Ddos.

O ataque conhecido como DoS (Denial of Service), ou negação de serviço, consiste em disparar de forma ininterrupta pacotes contra um determinado servidor, de forma a exceder a capacidade de resposta do mesmo, com a intenção de deixá-lo fora do ar [44].

O ataque DDoS é uma evolução do DoS e significa Distributed Denial of Service, ou seja, negação distribuída de serviço.

Enquanto no DoS, uma máquina é utilizada para enviar os pacotes ao servidor atacado, na modalidade DDoS o hacker utiliza várias maquinas para atacar o servidor que deverá ser derrubado.

Para que isto seja possível, é necessário que as várias máquinas que vão ser utilizadas para realizar o ataque estejam sob controle do hacker. Para controlar uma máquina na rede, o hacker pode se utilizar de ferramentas conhecidas genericamente como *Trojan Horse* (Cavalo de Tróia).

Um Trojan Horse é um programa que trabalha no sistema cliente-servidor, onde a máquina invadida fica com o software servidor e o hacker invasor possui o

software cliente. Desta forma é possível controlar a distância um outro computador, através de uma porta aberta, disponível ao invasor.

Normalmente um usuário de computador não aceita conscientemente um Trojan Horse em sua máquina. O Trojan é instalado sem que o usuário invadido tenha conhecimento da invasão.

Para que isto possa acontecer, o mais comum é que, o hacker envie o Trojan através de algum artifício de disfarce, como por exemplo, um arquivo anexo em um email, que ao ser aberto, instale de forma secreta o Trojan na máquina invadida.

Estas máquinas controladas podem ser divididas em Masters e Agentes, participando de um modo organizado hierarquicamente do ataque, que pode ser dividido nas seguintes etapas:

- Numa primeira etapa várias máquinas conectadas à rede são pesquisadas para que se analise quais podem ser utilizadas. As máquinas que estão vulneráveis à invasão são as escolhidas e, preferencialmente, devem possuir acesso rápido à Internet, e permanecerem conectadas constantemente à rede.
- Na etapa seguinte, as máquinas selecionadas serão divididas entre Master e Agentes. O master será o host que normalmente não é monitorado pelos administradores da rede em que se localiza. O agente será um host que tem acesso rápido à Internet. O software utilizado para DDoS é composto de duas partes: um software cliente, que é instalado no agente e um software servidor, que é instalado no master. Este relacionamento normalmente é de 1 para N, ou seja, um único master, enviará comandos para vários agentes.

- A etapa final é a concretização do ataque. O hacker envia parâmetros de ataque para os hosts master que ele controla, e estes por sua vez enviam os comandos para os agentes, que iniciarão os disparos de pacotes contra o host vítima do ataque.

O ataque pode ser melhor exemplificado através do seguinte esquema:

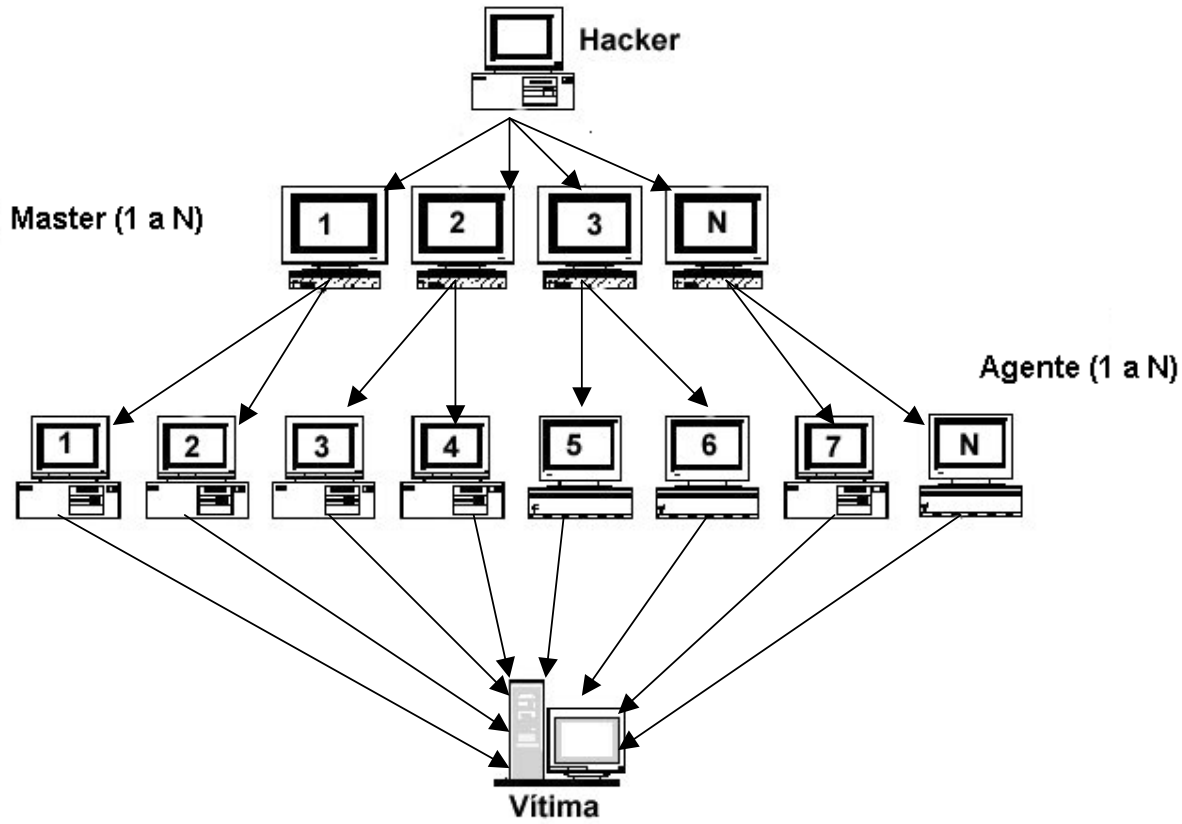

Figura 5.1: O ataque DdoS.

Existem ferramentas especificamente desenvolvidas para viabilizar um ataque DDoS. Apesar das diferenças técnicas entre estes, todos os softwares basicamente trabalham no esquema citado, entre os quais destacamos: Fapi, Blitznet, Trinoo, TFN, Stacheldraht, Shaft, TFN2K, Trank e Trinoo Win Version.

5.3.4 – IP Spoofing.

O ataque IP Spoofing é baseado num disfarce. O hacker altera o IP de origem para se passar por uma máquina conhecida (um IP reconhecido) e enganar a máquina alvo do ataque [45].

Uma análise mais profunda vai revelar que esta forma de ataque não é tão simples como parece, isto porque somente alterar o IP de origem, não torna o ataque possível. Além disto, o hacker não terá acesso aos pacotes respondidos pela máquina vítima, pois estes estarão endereçados ao IP de origem (falsificado).

Para que uma conexão TCP seja considerada correta, é estabelecido um número para seqüenciar a troca de pacotes. A checagem de possíveis erros através do mecanismo ACK (Acknowledgement), é baseada neste número escolhido.

Para exemplificar melhor, vamos adotar a existência de um host A e de um host B. Quando uma conexão é iniciada, o host A (solicitante) envia uma seqüência de números embutida nos identificadores do pacote, dirigido ao host B. O host B (solicitado), responde então com sua seqüência de números em um ACK. Este ACK, será o número gerado por A, adicionado a 1. Da mesma forma o ACK de A, será um número gerado por B, adicionado a 1.

A grande dificuldade para o hacker, é que este número, utilizado para confirmação do ACK, é gerado arbitrariamente. Portanto, não é possível saber qual será o número enviado pelo computador que o hacker quer enganar, para poder responder o ACK, correto.

Isto não significa que o ataque não possa ser perpetrado. Existem algumas soluções para encontrar o número correto [46]:

- O hacker pode fazer várias requisições com o IP de sua máquina, para assim receber pacotes do computador que deseja invadir e com muita

análise dos pacotes recebidos, entender o mecanismo pelo qual o computador contatado gera a seqüência de números e prever qual será o número enviado durante as conexões.

- Esta análise pode ser facilitada com a utilização de programas que analisam as seqüências para estabelecer a fórmula utilizada. Para complicar a situação de quem anseia por segurança, estes programas estão disponíveis na Internet e tem seu código fonte escrito em C, o que os torna portáveis para várias plataformas. Entre estes se pode citar: Spoofit, Mendax, Seq_number, Ipspoof, etc.

Além da dificuldade imposta pela geração do número de sequência, existem outras. Voltando ao exemplo anterior, vamos supor que o host A queira se conectar ao host B, porém como se ele fosse o host C. O host A, vai enviar como endereço de origem o endereço do host C, o que significa dizer que durante a negociação da conexão, o host B, vai responder para o endereço do host C. Isto produz mais duas dificuldades ao invasor:

1. Ele não obterá resposta do host B. Enquanto o protocolo de inicialização não estiver concluído, as respostas do host B, serão direcionadas para o host C.
2. Se o host C receber algum pacote do host B, o host C responderá ao host B. Isto não pode acontecer para que não exista nenhum problema durante a conexão.

Infelizmente, estes problemas também podem ser superados pelo hacker, que pode sobrecarregar o host C, para que este não responda a nenhum pacote enviado pelo host B, utilizando técnicas como a já demonstrada no item 5.3.3.

Desta forma, enquanto o host C é atacado, e não consegue responder a nenhuma solicitação que lhe é enviada, o host A negocia com o host B, e após o processo de reconhecimento estar realizado, pode operar livremente, tendo acesso ao host B, como se realmente fosse o host C.

Apesar de muito trabalhoso, o IP Spoofing não só é possível, como também é uma das técnicas mais utilizadas. Pode-se citar como exemplo o ataque realizado por Kevin Mitnick, que ganhou notoriedade mundial e alguns anos de cadeia após praticar uma invasão utilizando este método.

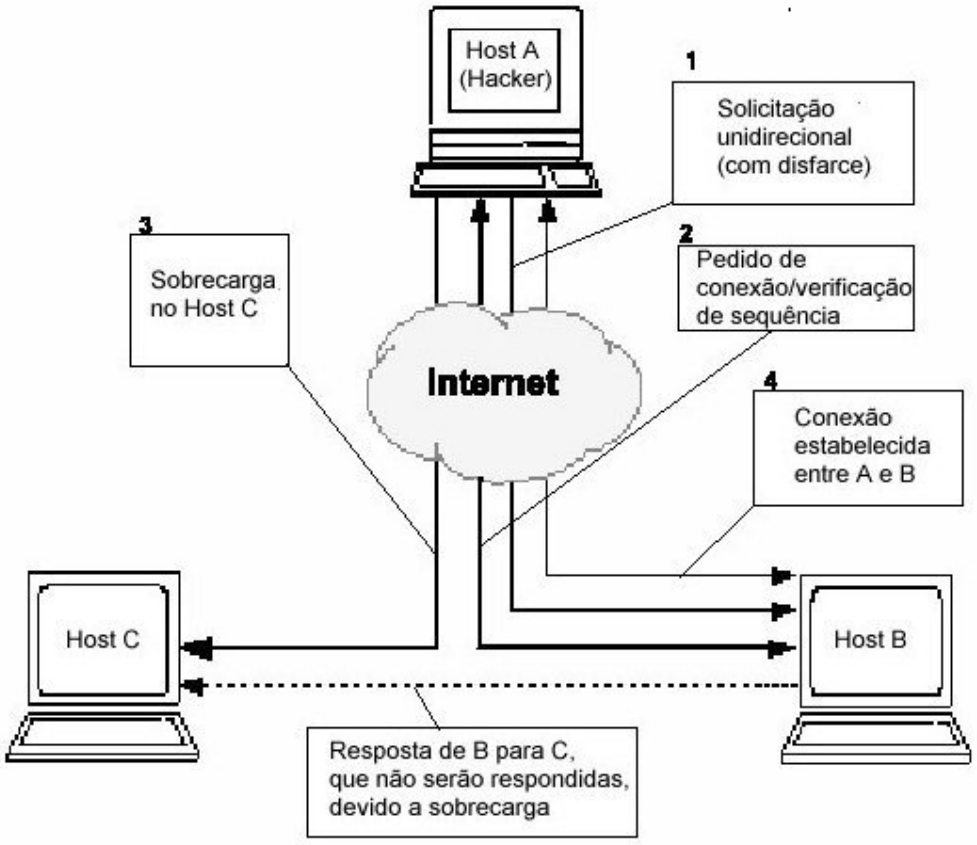

Figura 5.2: A seqüência do ataque IP Spoofing.

CAPÍTULO 6

Fundamentos de segurança na transmissão de dados

Este capítulo mostra os principais mecanismos de defesa à segurança dos dados que trafegam via rede.

A importância desde capítulo é justificada, uma vez que é necessário o conhecimento destes fundamentos para então conhecer as ferramentas que implementam estes mecanismos.

6.1 – Criptografia.

A palavra criptografia é originária do grego e significa “escrita escondida”, kriptós = escondido e grápho = grafia, ou seja, é a arte ou ciência de escrever em cifra ou em códigos, de modo a tornar o texto original em um texto criptografado, indecifrável para quem não conhecer o sistema de criptografia adotado.

Para o estudo da criptografia, alguns conceitos são básicos:

- Criptografia, função ou mecanismo pelo qual o texto original é transformado em um texto cifrado, também denominado texto encriptado ou ainda criptografado.
- Decriptação, função ou mecanismo pelo qual se obtém o processo inverso, ou seja, a partir de um texto criptografado, é obtido o texto original. Este processo também é denominado decriptografia.

- Algoritmo de cifra, ou ainda algoritmo de criptografia, é o método criptográfico utilizado, que a partir de uma chave escolhida, e aplicado ao texto original, produz o texto criptografado. O Algoritmo deve possuir as seguintes características:
  a) O texto criptografado só pode ser revertido no texto original, apenas pelo possuidor da chave.
  b) Não pode ser decifrado sem a chave.
  c) Mantém-se seguro, mesmo que sua forma seja divulgada.
  d) Oferece um resultado o mais aleatório possível, de modo a dificultar a identificação do padrão utilizado.
- Chave: a chave criptográfica tem um conceito semelhante ao de uma chave comum. Da mesma forma que a chave comum permite fechar e abrir portas. A chave criptográfica é o segredo que submetido ao algoritmo criptográfico permite a criptografia ou a decriptografia do texto. Segundo Shirey: *"É um parâmetro de entrada para o algoritmo criptográfico"* [47].

Basicamente, podemos adotar o seguinte esquema para ilustrar a criptografia:

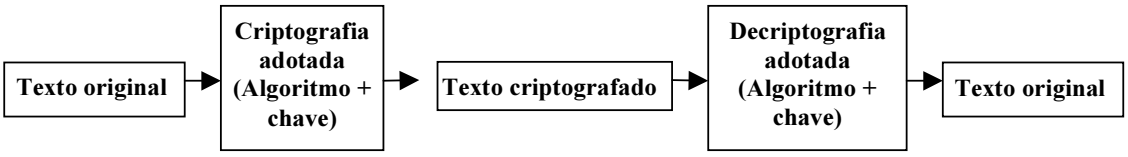

Figura 6.1: Criptografia / decriptografia.

No esquema descrito, o texto original (plaintext) ou texto claro (cleartext), é transformado através de uma função (método de criptografia) no texto criptografado, também denominado, texto cifrado (ciphertext).

Esta função é o algoritmo de criptografia, que juntamente com a chave adotada permite a transformação do texto original em texto cifrado.

Desta forma, o texto criptografado somente poderá ser transformado novamente no texto original através do método de decriptografia (algoritmo + chave), por quem conhecer a chave para a decriptografia, que pode ou não, ser a mesma utilizada para criptografia.

Pode-se também usar uma notação, através de uma fórmula, para descrever o mesmo esquema, sendo:

P → Texto normal.

k → Chave criptográfica.

C → Texto criptografado.

E → Função para criptografia do texto

D → Função para decriptação do texto criptografado.

O texto criptografado é a função da chave, aplicada ao texto normal : $C=E_k(P)$.

A função da chave aplicada ao texto criptografado permite obter o texto original : $P=D_k(C)$.

Finalizando pode-se ter $D_k(E_k(P)) = P$ [4].

A criptografia é tão antiga quanto a própria escrita. Já estava presente no sistema de escrita dos egípcios. Os romanos também utilizavam códigos secretos para comunicar planos de batalha. Um dos métodos conhecidos de criptografia é a cifra de César, atribuída ao imperador Júlio César.

A tecnologia de criptografia não mudou muito até meados do século XX, tomando novo impulso com o advento da Segunda Guerra Mundial, e logo a seguir, com a invenção do computador.

Durante a Segunda Guerra, os ingleses ficaram conhecidos por seus esforços para quebra de códigos criptográficos utilizados pelos inimigos. Na verdade, esse trabalho criptográfico formou a base para a ciência da computação moderna.

De um modo geral, a criptografia sempre foi mais utilizada pelos militares, para proteger suas comunicações secretas e confirmar mensagens sigilosas, as quais nas mãos do exército inimigo, poderiam determinar a derrota das tropas que estavam se comunicando.

Tradicionalmente podemos classificar os métodos criptográficos em cifras de substituição e cifras de transposição [48].

6.1.1 – Cifras de Substituição.

Neste método criptográfico ocorre uma troca de bits, caracteres ou grupos de caracteres. O exemplo mais antigo que se pode comentar é a já citada cifra de César.

Neste algoritmo as letras do alfabeto, são deslocadas em três posições, de modo que a letra “A” seja representada pela letra “D”, a letra “B” pela letra “E” e assim sucessivamente.

Desta forma a palavra CRIPTOGRAFIA, após o processo de criptografia, será escrita como FULSWRJUDILD. Na cifra de César, podemos dizer que a chave criptográfica utilizada no exemplo é igual a 3, outras chaves poderiam ser aplicadas, com um deslocamento diferente de 3.

O método utilizado no exemplo citado foi a **Substituição Monoalfabética**, pois cada letra foi simplesmente trocada por outra. Existem outras formas de substituição:

- **Substituição por deslocamentos:** Uma evolução da substituição monoalfabética, a chave não indica um único deslocamento, mas as letras têm diferentes posições trocadas. Exemplo: Para uma chave igual a 030711, a primeira letra avançara 03 posições, a segunda 07 e a terceira 11 posições e assim sucessivamente.

- **Substituição Monofônica:** Também uma evolução da substituição monoalfabética, a chave não indica um único deslocamento, mas é utilizada uma tabela de correspondência entre as letras do texto original e as letras do texto criptografado para aumentar o grau de confiabilidade do método, pois desta forma, não existe uma linearidade da substituição.

- **Substituição Polialfabética:** É utilizada a combinação de várias substituições monoalfabéticas, utilizando grupo de caracteres, e não somente um caractere individual.

6.1.2 – Cifras de Transposição.

Ao contrário da cifra de substituição, que troca o caractere original por outro, porém o mantém em sua posição original, a cifra de transposição, preserva o caractere original, mas sua posição original é trocada.

Desta forma, utilizando a mesma chave do exemplo anterior (3), a palavra cifrada ficaria como CPGFRTRIIOAA.

Demonstração:

(3 colunas)

1	**2**	**3**
C	R	I
P	T	O
G	R	A
F	I	A

Tabela 6.1: Exemplo de transposição.

O texto foi escrito, subdividido em colunas e cada coluna passou a ser descrita como uma parte da linha. Primeiro vem as letras da coluna 1, depois da coluna 2 e por fim as letras da coluna 3.

Assim sendo, as letras originais foram mantidas, porém sua ordem foi trocada, dificultando a quem não conhece o método obter o texto original.

6.1.3 – Criptoanálise.

Criptoanálise é a arte, ou a ciência de analisar textos criptografados e, mesmo sem o conhecimento prévio do método empregado e da chave utilizada, obter o texto original.

O criptoanalista primeiramente deve determinar qual o método utilizado, se é o de cifra, de substituição ou cifra de transposição. Isto pode ser feito através da análise dos caracteres utilizados na mensagem cifrada.

Do momento em que o criptoanalista consegue determinar o método utilizado, com um pouco mais de esforço, ele pode descobrir a chave utilizada e ir compondo o quebra-cabeça que o leve a obter o texto original.

O criptoanalista não parte de uma substituição de caractere por caractere aleatoriamente, método conhecido como ataque da força bruta (a brute force attack), para verificar qual caractere faz sentido, pois este método pode ser lento, mesmo com o uso do computador.

O método freqüentemente utilizado é uma análise das letras e dígrafos que mais ocorrem no idioma nativo da mensagem. Com esta técnica ele pode minimizar o trabalho para chegar à chave utilizada pelo algoritmo.

Muitos algoritmos criptográficos são de domínio público, porém a obscuridade está na chave utilizada. Ou seja, o método criptográfico pode ser conhecido, mas

isto não significa que uma mensagem criptografada com este método estará desprotegida, pois se a chave não for conhecida, não será possível reverter a mensagem criptografada na mensagem original.

Neste caso, o trabalho do criptoanalista será determinar a chave utilizada pelo algoritmo, sem a qual não é possível decifrar o código criptografado. Assim sendo, quanto maior o tamanho da chave utilizada, maior o número de combinações possíveis e, portanto, maior a dificuldade para se quebrar (descobrir) a mesma.

Segundo Tanenbaum: *"O fator de trabalho para decodificar o sistema através de uma exaustiva pesquisa no espaço de combinações da chave é exponencial em relação ao tamanho da chave"* [4].

6.2 – Criptografia de chave simétrica.

Neste conceito de algoritmo, a chave criptográfica utilizada para criptografar o texto original é a mesma que é utilizada para decriptografar o texto criptografado, como demonstrado na figura 6.2:

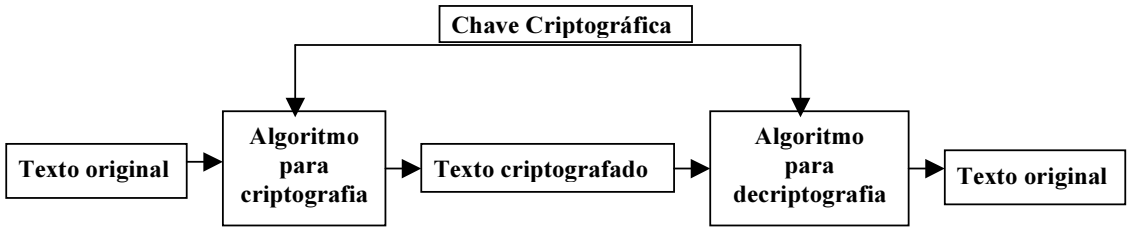

Figura 6.2: Criptografia simétrica.

Estes algoritmos também são denominados algoritmos de chave secreta, pois a segurança do método criptográfico está baseada no sigilo da chave utilizada.

Para que isto ocorra, apenas o emissor e o receptor da mensagem devem conhecer a chave utilizada. A chave que o emissor utiliza para criptografar o texto original é a mesma chave que o receptor utiliza para reverter o texto criptografado em texto original.

Um ponto fraco dos algoritmos de chave secreta é determinar como estas chaves vão ser estabelecidas de um modo seguro, para que apenas o emissor e o receptor as detenha. Este problema fica ainda mais evidenciado quando esta negociação para estabelecimento da chave ocorre através do uso de redes de computadores.

Se a criptografia está sendo proposta como uma forma de garantir o sigilo dos dados, como se pode garantir que o estabelecimento da chave secreta, antes da criptografia, estará a salvo de cair em poder de terceiros ?

Existem vários protocolos para a autenticação de usuários, a fim de estabelecer entre o emissor e o receptor uma senha secreta válida, entre o quais se pode citar:

- Protocolo de desafio-resposta.
- Protocolo de troca de chave de Diffie-Hellman.
- Protocolo do sapo de boca larga (KDC).
- Protocolo de Needham-Schroeder.
- Protocolo de Otway-Rees
- Protocolo Kerberos.

Para cada um dos protocolos, a exceção do protocolo Kerberos, existe uma forma de ataque que permite a um intruso obter a chave secreta e gerar informações, como se ele fosse o emissor ou receptor original.

Assim sendo, é possível dar razão a seguinte frase, que encontramos em Tanenbaum: *"Projetar um protocolo de autenticação correto é mais difícil do que parece"* [4].

6.2.1 – DES (Data Encryption Standard).

O DES [49] é um dos mais conhecidos algoritmos de chave secreta. Desenvolvido pela IBM, inicialmente trabalhava com uma chave de 128 bits, porém, sob influência da NSA (National Security Agency), passou a utilizar uma chave de 56 bits.

O DES utiliza várias etapas de criptografia e utiliza várias técnicas simultaneamente, entre elas a substituição, a transposição e o OU EXCLUSIVO. Estas técnicas são aplicadas bit a bit, o que garante que não ocorra correspondência de freqüência de caracteres.

O DES tem 19 estágios diferentes, sendo que 16 deles utilizam chaves diferentes, todas calculadas a partir da chave secreta original de 56 bits.

Apesar de toda esta complexidade envolvida o DES já não é seguro, existindo várias teorias para quebrá-lo. Segundo Tanenbaum [4]: *"O DES não deve ser mais usado para nada realmente importante".*

Por causa desta situação, novas aplicações surgiram para fortalecer o DES:

- DES Duplo, neste método de criptografia é utilizada a aplicação do algoritmo DES duas vezes, com o uso de duas chaves distintas. Esta técnica também se mostrou insegura, pois Merkle e Hellman, desenvolveram um ataque denominado meet-in-the-middle que torna esta aplicação insegura.

- DES Triplo, neste método também são utilizadas duas chaves, porém neste conceito, o texto é criptografado com a primeira chave, decriptografado com a segunda chave e novamente criptografado com a primeira chave. Este método é bem sólido, sendo utilizado comercialmente pela IBM.

6.2.2 – IDEA (International Data Encryption Algorithm).

O IDEA [50] é um algoritmo proposto por Lai e Massey em 1990, que utiliza uma chave de 128 bits, o que torna o algoritmo livre dos ataques conhecidos e dos quais o DES é suscetível.

Semelhante ao DES, ele é constituído de várias interações, sendo que para estas interações são utilizadas 52 chaves de 16 bits, derivadas da chave de 128 bits, 6 chaves para oito interações e 4 chaves para a transformação final.

O IDEA utiliza duas chaves, uma para a criptografia e outra para a decriptografia dos dados.

6.3 – Criptografia de chave assimétrica.

O conceito de criptografia de chaves assimétricas é muito mais recente que o simétrico. Enquanto a criptografia de chave simétrica existe com certeza, há mais de 2.000 anos, o conceito de chaves assimétricas surgiu em meados da década de 70.

Este conceito também é conhecido como Criptografia de Chave Pública / Privada, e foi proposto teoricamente por Diffie e Hellman, pesquisadores da Universidade de Stanford, tendo como base os seguintes requisitos [51]:

a) Uma chave é usada para criptografar o texto e outra para decriptografar.

b) É praticamente impossível, a partir de uma chave se chegar a outra.

c) Não é suscetível ao ataque da força bruta.

A criptografia de chave pública é uma técnica que usa um par de chaves assimétricas para criptografia e decriptografia. Cada par de chaves consiste de uma chave pública e uma chave privada.

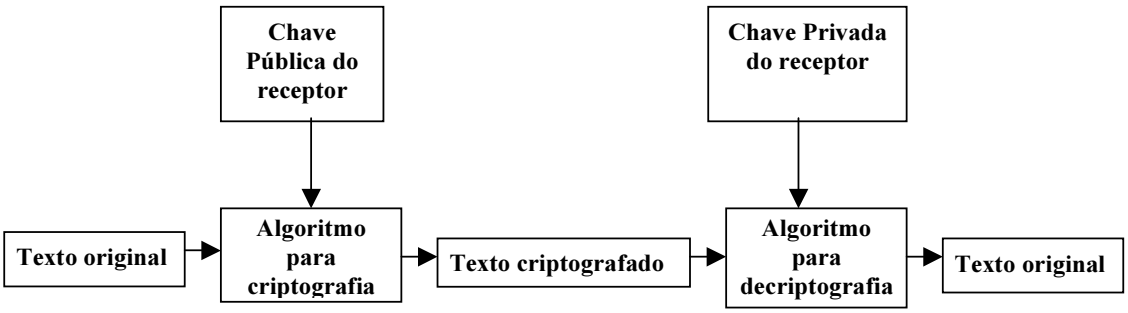

Figura 6.3: Criptografia assimétrica.

A chave pública é divulgada e distribuída amplamente. A chave privada nunca é distribuída; sempre é mantida em segredo.

Dados que são codificados com a chave pública só podem ser decifrados com a chave privada. Reciprocamente, dados codificados com a chave privada só podem ser decifrados com a chave pública. Desta forma, um dos grandes problemas da criptografia de chave simétrica é resolvido: A troca de chaves.

Enquanto na criptografia simétrica, existe a chance da chave ser capturada durante a transmissão; na criptografia de chave assimétrica, o problema é resolvido.

Não há problema em se distribuir a chave pública, porque atendendo aos requisitos citados, é muito difícil encontrar a chave privada, a partir da chave pública.

Esta assimetria é a propriedade que faz a criptografia pública ser amplamente difundida para autenticação e criptografia de dados, como forma de atender os vários requisitos para implementação de segurança na Internet.

Os conceitos matemáticos utilizados estão baseados na complexidade da teoria dos números, para os quais não existem soluções matemáticas eficientes, mesmo com o uso de computador.

Porém, a complexidade que garante a eficiência do sistema é a mesma que pode tornar o processamento lento, podendo tornar inviável o uso da mesma, se a chave escolhida, for muito grande.

6.3.1 – Algoritmo RSA.

O algoritmo RSA [52] foi criado por pesquisadores do MIT (Massachusetts Institute of Technology) Rivest, Shamir e Adleman em 1977, com a idéia de implementar um algoritmo seguro com uso de chaves assimétricas, a partir do princípio da teoria dos números [53].

Aqui será reproduzido um exemplo, dado que:

a) Serão gerados dois números primos p e q

   Normalmente o algoritmo trabalha com números primos extensos, normalmente 10^{100}. Porém para este exemplo, utilizaremos números pequenos. Assim sendo, aleatoriamente, serão utilizados:

   $p = 7$ e $q = 19$.

b) Para obter n, utiliza-se a fórmula: $n = pq$

   Desta forma: $n = 7x19 \rightarrow n = 133$.

c) Para obter *m*, utiliza-se a fórmula (*p* – 1) (*q* – 1)

Assim sendo: (7 - 1) (19 – 1) → 6 x 18 = 108 → *m* = 108

d) Para obter *e*, deverá ser gerado um número que juntamente com *m* apresente um MDC (Máximo Divisor Comum) igual a 1.

Como o *m* calculado é 108, serão testados números que satisfaçam a condição:

Para *e* = 2 (MDC de 2 e 108) = 2 (Não satisfaz)

Para *e* = 3 (MDC de 3 e 108) = 3 (Satisfaz)

Para *e* = 4 (MDC de 4 e 108) = 4 (Não satisfaz)

Para *e* = 5 (MDC de 5 e 108) = 1 (Satisfaz)

Desta forma o número escolhido para ser *e* = 5.

e) Encontrar *d*, a partir da fórmula: *de*=1+*zm*, desde que o *d* obtido seja um inteiro:

Se *de* = 1 + *zm*, então: *d* = (1 + *zm*) / *e*. Assim aleatoriamente, serão testados valores que atendam as exigências:

Para *z* = 0 → *d* = (1 + 0x108) / 5 → *d* = 1 / 5 → *d* = 0,2 (Não satisfaz)

Para *z* = 1 → *d* = (1 + 1x108) / 5 → *d* = 109 / 5 → *d* = 21,8 (Não satisfaz)

Para *z* = 2 → *d* = (1 + 2x108) / 5 → *d* = 217 / 5 → *d* = 43,4 (Não satisfaz)

Para *z* = 3 → *d* = (1 + 3x108) / 5 → *d* = 325 / 5 → *d* = 65 (Satisfaz)

Desta forma o número escolhido para ser *d* = 65.

f) Com estes valores podemos chegar às chaves:

Chave pública → *n* = 133 *e* = 5

Chave privada → *n* = 133 *d* = 65

g) Criptografando um texto com a chave pública, aplicando o algoritmo de criptografia $C = P^e \pmod n$

Para teste será utilizado o número 6 como texto normal:

$C = 6^5 \pmod{133} \rightarrow C = 7776 \pmod{133} \rightarrow C = 62$

Desta forma o texto normal 6 criptografado com a chave pública apresentará o texto criptografado 62.

h) Decriptografando o texto criptografado 62, com a chave privada, aplicando o algoritmo de decriptação $P = C^d \pmod n$

$P = 62^{65} \pmod{133}$

Mesmo para este exemplo, com valores pequenos o valor resultante de 62^{65} é muito alto, o que leva a necessidade de quebrar a função em vários passos:

$P = 62^{65} \pmod{133} \rightarrow 62 \times 62^{64} \pmod{133} \rightarrow 62 \times (62^2)^{32} \pmod{133} \rightarrow$

$62 \times 3844^{32} \pmod{133} \rightarrow 62 \times (3844 \pmod{133})^{32} \pmod{133} \rightarrow$

$62 \times 120^{32} \pmod{133}$

Esta simplificação da expressão deve ser aplicada novamente:

$P = 62 \times 120^{32} \pmod{133} \rightarrow 62 \times (120^2)^{16} \pmod{133} \rightarrow$

$62 \times (14400)^{16} \pmod{133} \rightarrow 62 \times (14400 \pmod{133})^{16} \pmod{133} \rightarrow$

$62 \times 36^{16} \pmod{133}$

Nova simplificação:

$P = 62 \times 36^{16} \pmod{133} \rightarrow 62 \times (36^2)^8 \pmod{133} \rightarrow$

$62 \times (1296)^8 \pmod{133} \rightarrow 62 \times (1296 \pmod{133})^8 \pmod{133} \rightarrow$

$62 \times 99^8 \pmod{133}$

Nova simplificação:

$P = 62 \times 99^8 \pmod{133} \rightarrow 62 \times (99^2)^4 \pmod{133} \rightarrow$

$62 \times (9801)^4 \pmod{133} \rightarrow 62 \times (9801 \pmod{133})^4 \pmod{133} \rightarrow$

$62 \times 92^4 \pmod{133}$

Nova simplificação:

$P = 62 \times 92^4 \pmod{133} \rightarrow 62 \times (92^2)^2 \pmod{133} \rightarrow$

$62 \times (8464)^2 \pmod{133} \rightarrow 62 \times (8464 \pmod{133})^2 \pmod{133} \rightarrow$

$62 \times 85^2 \pmod{133}$

Agora finalmente é possível a resolução:

$62 \times 7225 \pmod{133} \rightarrow 447950 \pmod{133} \rightarrow 6$

Ou seja, a partir do valor criptografado 62, pode-se obter o texto original 6.

6.4 – Message Digest.

A criptografia de chaves assimétricas, apesar de ser segura, como já vimos, demanda muito processamento. Assim sendo, ao invés de se criptografar uma mensagem inteira, pode-se utilizar uma técnica conhecida como Message Digest ou resumo de mensagem, para garantir a autenticidade da mensagem.

O Message Digest é o resultado obtido com a execução de um algoritmo hash em um texto, isto é, um sumário (conjunto de bits) gerado pelo algoritmo.

O Message Digest tem as seguintes propriedades:

- Não pode ser revertido. Durante a execução do algoritmo hash são aplicadas funções matemáticas que, por utilizar funções unidirecionais, torna impossível a partir do “Message Digest” chegar à mensagem origem.
- Um intruso não conseguiria criar um Message Digest com o mesmo valor.
- O Message Digest é uma representação condensada da mensagem.
- Além disso, a probabilidade de duas mensagens distintas terem o mesmo “Message Digest” é praticamente nula.

Figura 6.4: Esquema de message digest.

O fato de ser unidirecional é uma das diferenças básicas entre as funções de criptografia e funções de hash. Enquanto um texto criptografado pode ser revertido para a mensagem original, desde que aplicado o algoritmo e a chave correta, numa função de hash, qualquer saída resultante, não pode ser revertida para o texto original.

Assim o “Message Digest” é como uma impressão digital da mensagem. Ela garante a sua integridade, pois se algum bit for mudado durante a transmissão da mensagem, o cálculo feito pelo receptor para verificação irá detectar tal mudança.

Essa verificação consiste no receptor aplicar o mesmo algoritmo hash nos dados recebidos e comparar com o “Message Digest” recebido. Se eles forem iguais é certo que nenhuma mudança ocorreu.

Além disso, como será mostrado no próximo tópico, o Message Digest, pode ser utilizado para gerar uma assinatura digital.

Entre os principais algoritmos de hash pode-se citar o MD5 (Message Digest 5) [54] que é uma evolução do MD4, ambos criados por Ron Rivest do MIT. O MD5 é um algoritmo de 128 bits, ou seja, para qualquer mensagem aleatória, será produzido um hash de 128 bits.

Outro importante algoritmo é o SHA (Secure Hash Algorithm) [55], que foi desenvolvido pela NSA (National Security Agency). Ele gera uma função de hash de 160 bits.

6.5 – Assinatura Digital.

A assinatura digital existe a partir do conceito da criptografia assimétrica.

Como as chaves públicas e privadas são complementares, um texto criptografado por uma determinada chave privada, só poderá ser decriptografado com a chave pública correspondente.

Ao usar uma chave pública para decriptografar um texto cifrado, pode-se determinar a origem de quem gerou o mesmo, que somente poderá ser o detentor da chave privada.

A assinatura digital é utilizada para garantir a autenticação da transmissão, bem como, garantir o não-repudio. Isto porque, ao assinar digitalmente um texto, garante-se que apenas o detentor da chave privada poderia tê-lo feito.

O grande problema é o tempo de processamento necessário para que o processamento de todo o texto a ser criptografado / decriptografado possa ser realizado.

Este problema pode ser resolvido quando o “Message Digest” é utilizado, pois, ao invés de criptografar mensagens longas, utiliza-se uma função hash que possua um bloco de dados pequeno e de tamanho fixo, o que torna o processamento mais eficiente.

O message digest utilizado em conjunto com a chave privada do emissor, serve como garantia de autoria. Isto porque ao enviar uma mensagem e um Message Digest criptografado com a chave privada [56], está-se garantindo que aquela mensagem não pode ser negada.

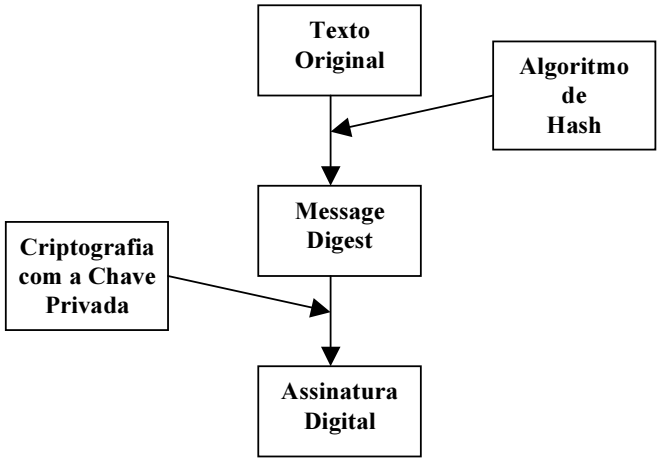

Figura 6.5: Esquema de assinatura digital.

Assim, o repúdio é inviabilizado, pois existe uma prova digital que aquela mensagem foi gerada pela pessoa que a assinou. Basta quem recebeu a mensagem decriptografar o Message Digest, utilizando a chave pública do emissor e submeter a mensagem original ao mesmo a algoritmo de hash e compará-las. Se ambos os resultados forem iguais, estará garantida a autenticidade da mensagem, desde que associada ao Certificado Digital que será abordado em breve.

A assinatura digital pode informar se a mensagem original foi adulterada, mas não informar o que foi adulterado.

Quanto aos aspectos legais, a CCJ (Comissão de Constituição Justiça e Cidadania) do Senado brasileiro, já aprovou em 23/05/2001 o projeto de lei de autoria do senador Lúcio Alcântara (PSDB-CE), que regulamenta o comércio eletrônico na Internet. Através desse projeto, a assinatura digital poderá ser utilizada nas mesmas situações que a lei requerer uma assinatura por escrito [57].

Para que uma assinatura digital não possa ser repudiada, é necessário o uso de um certificado digital, que será abordado no item 6.7 deste capítulo.

6.6 – MAC (Message Authentication Code).

Um MAC é um bloco de dados gerado a partir do uso de um processo criptográfico sobre a informação que se deseja autenticar.

Esta técnica envolve a utilização de uma chave secreta em conjunto com um algoritmo que é aplicado à mensagem e produz um bloco de dados de dimensão fixa conhecido por "Checksum criptográfico" [58] ou "Message Authentication Code" (MAC).

Por exemplo, usando o algoritmo de criptografia MD5, as chances de adivinhar um MAC correto é praticamente nula, 1 em 18.446.744.073.709.551.616.

A principal diferença entre o Message Digest e o MAC, é que enquanto o primeiro utiliza chave pública (assimétrica), o MAC utiliza chave secreta (simétrica).

6.7 – Certificado Digital.

O objetivo da existência de um certificado digital é garantir a autenticidade da chave pública de uma determinada entidade [59].

Um certificado digital é um conjunto de informações sobre uma entidade, a sua identificação e a sua respectiva chave pública. Estas informações devem ser utilizadas para gerar uma assinatura digital, que também deve fazer parte do certificado digital.

Quando uma outra entidade desejar obter a chave pública da entidade certificada, deverá solicitar seu certificado digital, verificar a validade da mesma e extrair a chave pública.

Um certificado deve ter as seguintes características:

- O nome do emissor de certificado
- A entidade para quem o certificado está sendo emitido.
- A chave pública da entidade certificada.
- Um time-stamp, ou seja, uma data de validade.

Outras características podem ser adicionadas ao certificado, como, por exemplo, dados pessoais, empresa onde trabalha, nível hierárquico, etc. Desta forma, o certificado pode ser utilizado para se verificar o que a pessoa certificada pode ou não aprovar, trazendo assim o conceito de autorização.

A assinatura digital é adicionada ao certificado por uma entidade em que as demais devem confiar: o emissor do Certificado. Este, por sua vez, é quem garante aos receptores da chave pública que ela pertence a quem diz ser o seu possuidor.

Assim, o certificado digital pode ser usado para, além da autorização, garantir a autenticação e não repúdio.

O certificado é assinado digitalmente pelo emissor, pois utiliza-se sua chave privada no certificado. A chave pública do emissor do certificado é distribuída livremente e, o emissor do certificado também possui um certificado, garantindo a autenticidade da sua própria chave pública.

Desta forma, o certificado digital é uma forma comum de ligar uma chave pública a um nome de usuário certificado.

Para que isto seja confiável, dois itens são importantes;

- O usuário certificado deve ter um controle rígido de sua chave privada. A mesma não pode ser acessada por outras entidades.
- A entidade certificada deve realmente ser quem diz ser ao retirar seu certificado. Neste caso, a entidade certificadora tem que possuir mecanismos eficazes para conferir e garantir a veracidade das informações.

Pode-se determinar diferentes tipos de certificados digitais:

- **Certificado de CA:** são certificados destinados a validar outros certificados, normalmente são assinados pela própria entidade certificadora, ou assinado por uma outra entidade.
- **Certificado de servidor:** são certificados que identificam o servidor, ligando o servidor à empresa certificada.

- **Certificado pessoal:** utilizado para certificar uma pessoa física, eventualmente pode ter alguns dados opcionais sobre a pessoa certificada.
- **Certificado de desenvolvedor de software:** certificado utilizado para validar assinaturas associadas a programas

6.8 – Autoridades de Certificação.

O sistema utilizado para a criação de certificados digitais, está baseado na existência de uma outra entidade denominada: emissora do certificado, ou autoridade de certificação, ou ainda CA (Certificate Authority).

Todo mecanismo de distribuição de chaves públicas, reconhecidas através da existência de um certificado digital, está apoiado na veracidade das informações apresentadas pelo detentor do certificado à entidade emissora do certificado digital.

Segundo Silva [60]: *"O certificado digital funciona com uma ´carteira de identidade digital´, a assinatura digital é equivalente a ´impressão digital´ e a autoridade de certificação pode ser comparada a um ´cartório digital´".*

A autoridade de certificação deve dispor de uma política de controle rígida, para garantir a veracidade das informações apresentadas pela entidade certificada, como por exemplo, a existência de documentos escritos e a presença física de um representante da mesma.

A autoridade de certificação deve dispor dos seguintes itens: [59]

- **Tecnologia:** Algoritmos criptográficos, protocolos de comunicação seguros e normas de segurança.

- **Infra-estrutura:** Sistemas seguros, suporte aos clientes e instalações capacitadas.

- **Experiência:** Conhecimento da área de atuação, credibilidade no mercado e conhecimentos dos aspectos legais que envolvam segurança.

6.9 – Um exemplo teórico.

No exemplo seguinte cada conceito visto anteriormente é empregado passo-a-passo para demonstrar o que cada item acrescenta em termos de segurança, seus pontos falhos e como se complementam.

6.9.1 – Definições:

Usuário-A: Uma entidade que representa algum dos componentes do Comércio Eletrônico, empresa, consumidor ou administração pública.

Usuário-B: Idem ao anterior.

Hacker: Uma entidade, como já foi definida no capítulo 4. Um intruso mal intencionado, que quer se apoderar das informações eletrônicas trocadas entre as entidades anteriores.

Criptografia: É usado o sistema criptográfico por chaves assimétricas.

Notação: A notação {texto}chave, indica que o que está entre chaves foi criptografado ou decriptografado utilizando a chave indicada.

6.9.2 – Autenticando o usuário.

Suponha que Usuário-A quer autenticar Usuário-B.

Usuário-B tem um par de chaves, uma pública e uma privada. Usuário-B envia a Usuário-A a chave pública dele.

Usuário-A gera uma mensagem aleatória e então envia isto a Usuário-B:

A → B	Mensagem aleatória

Figura 6.6: Mensagem de Usuário-A para Usuário-B.

Usuário-B usa a chave privada dele para codificar a mensagem e retorna a versão codificada para Usuário-A:

B → A	{Mensagem-Aleatória}Chave-privada-de-Usuário-B

Figura 6.7: Mensagem criptografada com a chave secreta de Usuário-B.

Usuário-A recebe esta mensagem e decifra a mesma, usando a chave pública de Usuário-B. Ele compara a mensagem decifrada com a mensagem original que enviou a Usuário-B; se elas forem iguais, ele saberá que está se comunicando com Usuário-B.

Um possível impostor não saberia a chave privada de Usuário-B e presumivelmente não poderia ter criptografado a mensagem aleatória gerada pelo Usuário-A.

Porém, do ponto de vista do Usuário-B, a menos que ele saiba o que está codificando exatamente, não é uma boa idéia codificar algo com sua chave privada e então enviar isto a outro alguém. Isto porque, qualquer um que tenha a chave pública de Usuário-B, poderá decodificar a mensagem.

Pode-se então, partir para um sistema mais bem elaborado, utilizando dois pares de chaves. As chaves pública e privada do Usuário-B e as chaves pública e privada do Usuário-A.

Assim sendo, o Usuário-B, poderia criptografar a mensagem utilizando a sua chave privada e em seguida criptografar novamente utilizando a chave pública do Usuário-A.

B → A	{{Mensagem-Aleatória}Chave-privada-de-Usuário-B} Chave-pública-de-Usuário-A

Figura 6.8: Mensagem duplamente criptografada.

O Usuário-A ao receber a mensagem, deve utilizar sua chave privada para decriptografar a mensagem, tendo certeza assim que ninguém mais pode ter lido a mesma, pois somente ele, que é o detentor da chave privada, pode decriptografar a mensagem. Em seguida ele utiliza a chave pública do Usuário-B e assim terá certeza que foi ele quem gerou a mensagem.

Porém, este sistema utilizando dois pares de chaves assimétricas, com dois processos de criptografia no envio e dois processos de decriptografia na recepção da mensagem, está descartado, dado que demanda muito processamento.

6.9.3 – Utilizando uma Assinatura Digital.

Usando um Message Digest, o Usuário-B pode se proteger. Ele calcula o Message Digest da mensagem aleatória enviada pelo Usuário-A, e então, codifica o resultado.

Assim, em vez de codificar a mensagem original enviada pelo Usuário-A, o Usuário-B pode criar um “Message Digest” e criptografá-lo.

Um Message Digest, utiliza a mesma mensagem aleatória, sendo mais rápido, e com as mesmas propriedades de autenticação.

Ele manda de volta o Message Digest codificado ao Usuário-A, e este pode calcular o mesmo Message Digest e pode autenticar o Usuário-B, decifrando sua mensagem e comparando os valores obtidos.

Esta técnica é a que está descrita como assinatura digital, no item 6.5. Neste exemplo, Usuário-B assinou uma mensagem gerada por Usuário-A.

A forma descrita também é perigosa, pois Usuário-B assinou um valor aleatório gerado externamente.

Para fortalecer esta técnica o ideal é que a autenticação parta de uma mensagem gerada por Usuário-B, como no exemplo a seguir:

A → B	Oi, é você Usuário-B?
B → A	Usuário-A, Sou eu Usuário-B
	{ digest[Usuário-A, Sou eu Usuário-B] } Usuário-B-chave-privada

Figura 6.9: Mensagem assinada digitalmente.

Quando usar este protocolo, Usuário-B sabe qual a mensagem que está enviando a Usuário-A, não existindo problemas em assinar a mensagem. Ele envia a versão sem criptografia da mensagem, e a versão assinada da mensagem.

6.9.4 – Utilizando Certificado Digital.

Como Usuário-B pode distribuir sua chave pública de um modo confiável?

A → B	Oi
B → A	Oi, sou eu Usuário-B, Usuário-B-chave-pública
A → B	confirme
B → A	Usuário-A, Sou eu Usuário-B
	{ digest[Usuário-A, Sou eu Usuário-B] } Usuário-B-chave-privada

Figura 6.10: Envio da chave pública de Usuário-B para Usuário-A.

Com este protocolo, qualquer pessoa pode se passar por Usuário-B. Apenas é necessário ter uma chave pública e privada.

Alguém pode se passar por Usuário-B e enviar suas chaves para Usuário-A e este não poderá saber se quem enviou as chaves é ou não Usuário-B.

Para resolver este problema, é usado na Internet o certificado digital (item 6.7).

Todo o mundo pode examinar o certificado de Usuário-B para ver se é Usuário-B mesmo, ou se é algum intruso tentando assumir o papel de Usuário-B.

Desta forma:

A → B	Oi
B → A	Oi, sou eu Usuário-B, Usuário-B-certificado
A → B	Confirme
B → A	Usuário-A, Sou eu Usuário-B { digest[Usuário-A, Sou eu Usuário-B] } Usuário-B-chave-privada

Figura 6.11: Envio do certificado digital de Usuário-B para Usuário-A.

Agora, quando o Usuário-A receber a primeira mensagem de Usuário-B, ele pode examinar o certificado, conferir a assinatura, usando o Message Digest e a chave pública de Usuário-B, e então conferir se o Usuário-B é realmente quem diz ser.

Se um intruso qualquer, (Hacker), tentar se passar por Usuário-B, acontecerá o seguinte:

A → H	Oi
H → A	Oi, sou eu Usuário-B, Usuário-B-certificado
A → H	Confirme
H → A	????

Figura 6.12: Hacker denunciado pelo certificado digital.

Hacker não pode satisfazer o Usuário-A na mensagem final. Hacker não tem a chave privada de Usuário-B, assim sendo, ele não pode construir uma mensagem que Usuário-A acreditará vir de Usuário-B.

6.9.5 – Combinando Criptografia Simétrica e Assimétrica.

Uma vez que Usuário-A autenticou Usuário-B, ele pode agora enviar mensagens que somente Usuário-B poderá decodificar:

A → B	{chave-assimétrica}Usuário-B-chave-pública

Figura 6.13: Troca de chave simétrica, com uso de chaves assimétricas.

O único modo para ler a mensagem em segredo é decifrando a mensagem com a chave privada de Usuário-B. A privacidade é um dos objetivos da criptografia de chave pública.

A comunicação entre Usuário-A e Usuário-B pode até ser observada, porém ninguém além de Usuário-B poderá ler a mensagem criptografada.

Esta técnica é utilizada para implementar segurança na Internet, a partir do conceito de criptografia simétrica.

Usuário-A sabe a chave simétrica, porque ele gerou a mesma antes de enviá-la ao Usuário-B. Por sua vez, Usuário-B acessa a chave simétrica, porque utiliza sua chave privada para decifrar a mensagem de Usuário-A.

Como ambos compartilham a chave simétrica, eles podem iniciar um algoritmo de criptografia simétrica e então iniciar o envio de mensagens criptografadas a partir desta nova chave secreta.

Desta forma, técnicas de criptografia assimétrica e simétrica estarão sendo utilizadas conjuntamente, a fim de garantir a integridade das informações trocadas através da Internet, como no exemplo a seguir:

A → B	Oi
B → A	Oi, sou eu Usuário-B, Usuário-B-certificado
A → B	Confirme
B → A	Usuário-A, Sou eu Usuário-B { digest[Usuário-A, Sou eu Usuário-B] } Usuário-B-chave-privada
A → B	Ok Usuário-B, aí vai uma chave simétrica {chave simétrica} Usuário-B-chave-pública
B → A	{texto}chave-simétrica

Figura 6.14: Combinando chaves simétricas e assimétricas para criptografia.

Como Hacker não pode descobrir a chave simétrica que Usuário-A e Usuário-B estabeleceram, ele não pode ter acesso às informações que Usuário-A e Usuário-B, trocam entre si, pois estas estão criptografadas pela chave simétrica.

Mesmo assim Hacker pode interferir na conversação danificando a comunicação, apenas com o intuito de prejudicar a troca de mensagens entre Usuário-A e Usuário-B.

Por exemplo, se Hacker estiver “ouvindo” a comunicação entre Usuário-A e Usuário-B, ele pode intermediar a informação interceptando, de um lado para outro, de forma inalterada, e a partir de um ponto, danificar certas mensagens, conforme demonstrado na figura 6.15:

A → H	Oi
H → B	Oi
B → H	Oi, sou eu Usuário-B, Usuário-B-certificado
H → A	Oi, sou eu Usuário-B, Usuário-B-certificado
A → H	Confirme
H → B	Confirme
B → H	Usuário-A, Sou eu Usuário-B { digest[Usuário-A, Sou eu Usuário-B] } Usuário-B-chave-privada
H → A	Usuário-A, Sou eu Usuário-B { digest[Usuário-A, Sou eu Usuário-B] } Usuário-B-chave-privada
A->H	Ok Usuário-B, aí vai uma chave simétrica {chave simétrica} Usuário-B-chave-pública
H->B	Ok Usuário-B, aí vai um chave simétrica {chave simétrica} Usuário-B-chave-pública
B->H	{texto}chave simétrica
H->A	erro[{texto}chave simétrica]

Figura 6.15: Hacker introduz um erro na mensagem de Usuário-B para Usuário-A.

Hacker atravessa os dados sem modificação até Usuário-A e Usuário-B compartilharem uma chave simétrica.

Então Hacker falsifica a mensagem do Usuário-B a Usuário-A introduzindo um erro. Até este ponto Usuário-A confia em Usuário-B, assim ele pode acreditar na mensagem adulterada e pode tentar usá-la.

Neste exemplo, Hacker não conhece a chave simétrica, tudo que ele pode fazer é danificar os dados que forem codificados com a chave secreta.

6.9.6 – Utilizando o MAC.

Para prevenir este tipo de dano, Usuário-A e Usuário-B podem introduzir um código de autenticação de mensagem (MAC) no protocolo.

MAC = checksum[texto, chave simétrica]

Figura 6.16: Utilizando Message Authentication Code.

O MAC é enviado em conjunto com a mensagem de Usuário-A para o Usuário-B. A partir daí, Usuário-B gera também um MAC e verifica se coincide com o que chegou juntamente com a mensagem.

Como apenas Usuário-A e Usuário-B conhecem a chave secreta, Usuário-B pode descobrir se a mensagem enviada por Usuário-A, é legítima ou foi adulterada.

O algoritmo de Message Digest descrito anteriormente no item 6.4 tem as propriedades certas para construir uma função de MAC :

MAC = Digest[texto, chave simétrica]

Figura 6.17: Utilizando um algoritmo de Message Digest para gerar um MAC.

Como Hacker não conhece a chave simétrica, ele não pode calcular o valor correto do MAC.

Até mesmo se Hacker falsificar mensagens aleatoriamente, a chance de sucesso é desprezível.

Desta forma todos os recursos vistos anteriormente podem ser combinados para garantir a segurança das mensagens transmitidas, como visto na figura a seguir:

A → B	Oi
B → A	Oi, sou eu Usuário-B, Usuário-B-certificado
A → B	Confirme
B → A	Usuário-A, Sou eu Usuário-B { digest[Usuário-A, Sou eu Usuário-B] } Usuário-B-chave-privada
A → B	Ok Usuário-B, aí vai um chave simétrica {chave simétrica} Usuário-B-chave-pública
A → B	{texto,MAC}chave simétrica

Figura 6.18: Utilizando todos os recursos descritos.

Hacker pode até se intrometer nas mensagens, porém o cálculo do MAC revelará sua intromissão. Quando Usuário-A ou Usuário-B descobrirem o falso MAC terminarão a comunicação.

CAPÍTULO 7

Ferramentas para implementar segurança na transmissão de dados

---

Este capítulo mostra algumas das principais ferramentas que possibilitam estabelecer uma conexão segura num meio inseguro como a Internet, para viabilizar o comércio eletrônico.

7.1 – Política de segurança.

O estabelecimento de uma política de segurança é vital para garantir a segurança das informações.

A política de segurança é determinada pela administração da informática na empresa e, de acordo com as decisões tomadas pela administração, são determinados vários fatores: grau de segurança, funcionalidade dos serviços, facilidade de utilização, quantidade de uso, etc [61].

Para o estabelecimento de uma política de segurança é necessário prioritariamente definir quais são as metas de segurança que se deseja atingir.

Estas metas podem ser definidas através dos seguintes critérios, extraídos da RFC 2196 [62]:

- **Serviço oferecido x Segurança.** O simples fato de oferecer um serviço na rede ao usuário implica em riscos para a segurança. É necessário

mensurar se o benefício resultante do serviço oferecido é superior ao risco inerente do serviço disponível.

- **Facilidade de uso x Segurança.** A implementação de mecanismos de segurança traz dificuldades de uso ao usuário do sistema. A simples adoção de uma senha já traz algum desconforto. Quanto maior for o grau de segurança que se deseja obter, concomitantemente, maior será o grau de dificuldade de uso do sistema.

- **Custo da Segurança x Risco.** A implementação de mecanismos de segurança traz custos financeiros adicionais ao orçamento da informática. Há que se contar também o custo de perda de desempenho do sistema ao se implementar rotinas de segurança e do aumento das dificuldades de uso impostas por estes mecanismos. A análise destes custos em relação aos riscos envolvidos, também deve ser analisada, numa típica relação custo x benefício.

Para que a política de segurança possa ser aplicada com o sucesso esperado, é necessário o envolvimento de várias pessoas dentro da organização, sendo que estas pessoas devem ter o devido respaldo por parte da administração da organização para a efetiva aplicação da política.

Por esta ótica, pode-se dizer que, dentre as pessoas que devem estar envolvidas no estabelecimento da política de segurança, deve-se começar pelo responsável pela administração da organização. Do outro lado da pirâmide organizacional, os usuários do sistema devem estar conscientes da necessidade de

cumprir as metas estabelecidas, e estarem cientes das possíveis punições, caso estas metas não sejam atingidas.

Além destes, obviamente, devem fazer parte do estabelecimento da política de segurança, o administrador da rede e o corpo técnico da área de informática, sendo que, dentro da área de informática, deverá existir um grupo ou comissão formado para analisar os incidentes de segurança que possam ocorrer.

A política de segurança deve estabelecer basicamente:

- As especificações de hardware e software para que estejam compatíveis com a política de segurança.
- O grau de privacidade que os usuários deverão ter.
- O nível de acesso que os diferentes usuários poderão ter aos diversos serviços oferecidos.
- Definição das responsabilidades dos usuários, quanto à segurança do sistema.
- Definição de como será feito o controle e a autorização da realização de manutenções em sistemas e redes.
- Manutenção de uma constante verificação da eficácia da política de senhas.
- Garantia da efetividade do sistema de backup.
- Definição das regras que devem ser aplicadas ao firewall da organização e providências para garantir a aplicação destas regras.
- Formação de uma equipe para registrar, analisar e tomar as devidas providências em incidentes que venham a transgredir a política de segurança.

Muitas vezes, quando se vai auditar o sistema de segurança, é normal que os auditores partam do que está estabelecido na política de segurança, para verificar se os itens estão sendo cumpridos, conforme determinado.

Em Silva [60] encontramos que *"A necessidade de auditoria é justificada para que se possa avaliar a existência e a adequação de uma política ampla que defina a postura da organização para o tratamento de suas informações"*.

Um item adicional que pode ser realizado pela equipe responsável pela segurança do sistema é realizar uma simulação de ataque hacker. A vantagem de se "atacar" o sistema sem se preocupar com a política de segurança, é que não se parte de nenhum pressuposto.

Sendo assim, diferentemente da auditoria que vai checar se a política está sendo ou não cumprida, a simulação de um ataque busca apenas falhas técnicas no sistema de segurança.

Para que a simulação seja proveitosa, ela deve ser realizada por alguém da equipe de segurança, que tenha conhecimentos técnicos suficientes para perpetrar o ataque e que tenha por objetivo, efetivamente, realizar uma invasão.

Como resultado, esta simulação deve produzir um relatório de diagnóstico de vulnerabilidades que deverá detalhar tecnicamente quais as vulnerabilidades críticas encontradas, que são aquelas que podem permitir uma invasão, e também mostrar quais não são críticas, mas podem vir a comprometer a segurança do sistema.

7.2 – Firewall.

Segundo Cheswick e Bellovin [63] temos que *"Genericamente pode-se definir firewall como um sistema utilizado para proteger a rede interna de acessos externos vindos da Internet"*.

Segundo Kalakota e Whisnton [16], também é possível definir firewall como sendo: *"O software ou hardware que apenas permite o acesso dos computadores externos à rede protegida, se estes possuírem determinadas características"* .

Normalmente um firewall permite aos usuários da rede interna terem acesso completo aos serviços disponíveis no exterior. No entanto, no sentido inverso, ou seja, da rede externa para a rede interna, o acesso somente é permitido para computadores selecionados através do nome, palavras chaves, endereço IP, URL, ou demais critérios.

O firewall é colocado entre a rede interna e a Internet, filtrando o tráfego de dados que passa entre as duas. Porém, o firewall pode realizar diversas funções, e não apenas filtrar o tráfego oriundo da rede externa. Como exemplo pode-se citar a função inversa, ou seja, o firewall pode restringir o acesso de algumas máquinas da rede interna à Internet.

Desta forma um firewall pode ser utilizado para implementar uma política de segurança ao realizar o bloqueio de acesso à Internet, ou a certos endereços e ainda registrar os eventos, fazendo um "log file" dos acessos realizados pelos usuários da rede interna.

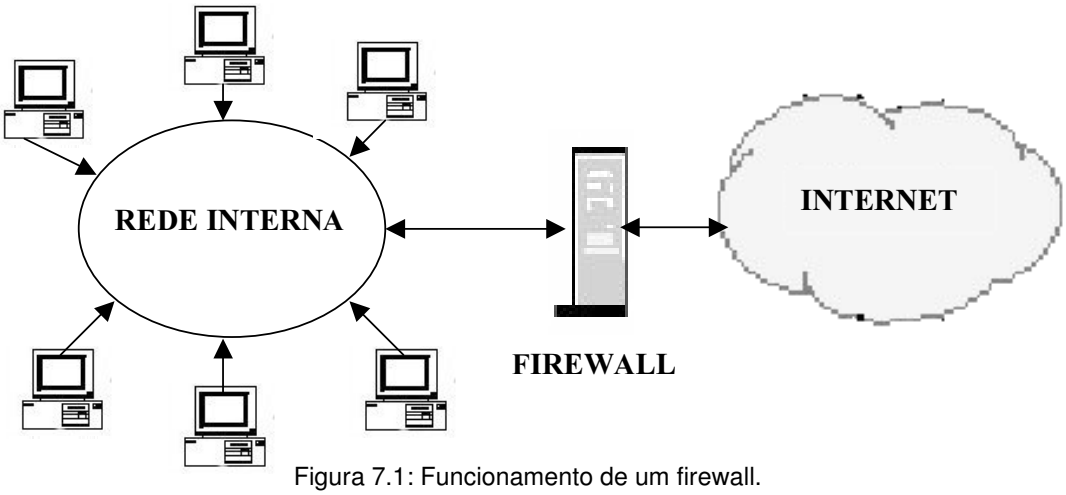

Figura 7.1: Funcionamento de um firewall.

O firewall pode realizar a filtragem baseada em vários critérios, além de realizar as seguintes funções:

- Filtragem por endereço de origem;
- Filtragem por endereço de destino;
- Filtragem pela combinação origem-destino;
- Filtragem por tipo de serviço (SMTP, FTP,HTTP, etc);
- Autenticação da origem dos acessos;
- Garantir a confidencialidade dos dados, a partir da criptografia dos dados.

Além das diferentes funções executadas por um firewall, também existem diversos tipos de firewalls [64], entre os quais pode-se citar:

7.2.1 – Simple traffic logging systems.

Sistemas que registram todo o tráfego que passa pelo firewall em um arquivo denominado log file, permitindo aos gestores da política de segurança, obter várias informações :

- Número de acessos por usuários;
- Bytes recebidos / enviados;
- Estatísticas sobre o tráfego de dados;
- URLs acessadas por usuários

Outras informações podem ser armazenadas para posterior verificação.

Este tipo de firewall não deve ser utilizado por administradores de rede que buscam um alto grau de segurança, pois sua utilização tem como objetivo básico o monitoramento do tráfego dos dados entre a rede interna e a Internet.

7.2.2 – IP packet screening routers.

Este tipo de firewall, também denominado Packet filtering gateway, funciona filtrando os pacotes de informação que passam pelo firewall.

O router firewall filtra os pacotes IP de entrada que passam por ele, permitindo ou não, o tráfego dos mesmos, de acordo com as regras programadas no router.

Esta filtragem é automática e entre as regras de filtragem mais comuns, pode-se citar:

- **Por protocolo:** Filtragem com base nos protocolos (TCP, UDP).

- **Por aplicação destino:** Controla o acesso por aplicação destino, restringindo o TCP/IP para apenas uma determinada porta, por exemplo.

- **Por IP:** Filtra por IP, restringindo o acesso a endereços desconhecidos, ou por tipos de endereço. Exemplo: permitir o acesso somente a domínios comerciais (.com).

7.2.3 – Hardened firewall hosts.

Neste tipo de firewall, exige-se que os usuários internos e externos acessem uma aplicação de segurança que deverá identificá-los, para somente então permitir o acesso a qualquer outro recurso da rede.

Normalmente este tipo de firewall é utilizado para proteger a rede interna de usuários externos, que não estejam habilitados a utilizá-la, mas, de forma genérica, pode ser utilizado para que nenhum usuário (interno ou externo) acesse uma máquina qualquer sem a devida permissão.

7.2.4 – Proxy application gateways.

Neste caso, os firewalls são utilizados conjuntamente com servidores proxy. O tráfego de dados é estabelecido através do proxy, que o repassa para os computadores da rede. O mesmo ocorre com o tráfego externo. Ou seja, primeiro é dirigido ao proxy, para depois ser transmitido aos computadores da rede.

O proxy é utilizado como um firewall em ambas as direções, filtrando o tráfego da rede interna para a externa, ou da forma contrária, filtrando os pacotes de dados vindos da rede externa para a interna.

Qualquer que seja o tipo de firewall utilizado, a eficiência deste sistema é inerente a dois fatores básicos: A capacidade dos técnicos que programam e operam o firewall e a política de segurança estabelecida na empresa.

Também deve-se ter em mente que um firewall não é um recurso que por si só garante segurança contra qualquer tipo de invasor, conforme advertência encontrada em [65]: *"Um firewall não pode ser a única linha de defesa, além do que eles protegem apenas contra ataques externos, nada podendo fazer contra ataques que partam de dentro da rede*".

7.3 – O protocolo IPSec.

O IPSec (IP Security) é um conjunto de padrões e protocolos que define as especificações de autenticação, integridade e confidencialidade, sendo assim uma extensão do protocolo IP, definido através da RFC 2401 [66].

Estas especificações determinam dois mecanismos que visam tornar o IP um protocolo seguro, o Authentication Header e o Encapsulating Security Payload.

7.3.1 – Authentication Header.

O Authentication Header, como a própria tradução indica, destina-se a providenciar mecanismos para autenticação da origem de um pacote IP. Também providencia garantias de integridade do seu conteúdo.

Próximo cabeçalho	Tamanho do módulo	Reservado
Índice de parâmetros de segurança (SPI)		
Número de seqüência		
Dados de autenticação		

Figura 7.2: Formato do cabeçalho de Autenticação (AH).

O SPI está presente no AH e no ESP e é o mecanismo que permite a comunicação entre as entidades, especificando todo o conjunto de segurança utilizado: Algoritmo criptográfico, chaves utilizadas, time-stamp, etc. Desta forma, o host que vai iniciar uma comunicação envia estas informações ao host destino e aguarda o retorno do SPI do host destino.

7.3.2 – Encapsulating Security Payload.

O Encapsulating Security Payload providencia confidencialidade dos pacotes IP, criptografando o conteúdo da área de dados.

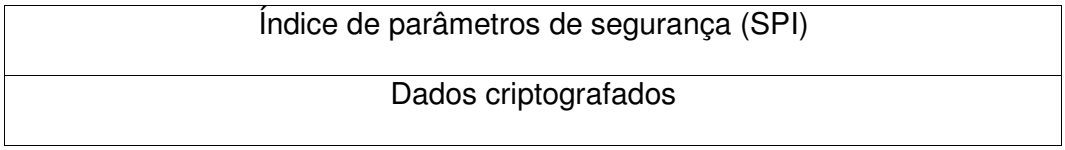

Figura 7.3: O encapsulating security payload.

7.3.3 – Funcionamento do IPSec.

O protocolo IPSec permite construir túneis seguros sobre redes inseguras, uma vez que os pacotes criptografados enviados por um host que utiliza IPSec, somente poderão ser decriptografados e lidos por um host que também utilize este protocolo. Entretanto, o IPSec deve fazer parte do software que implementa a camada de rede, sendo que todos os sistemas operacionais envolvidos devem suportá-lo.

Segundo a RFC 2401 [66] existem duas implementações do protocolo IPSec. O modo transporte e o modo túnel: no modo transporte, o protocolo oferece proteção somente para os protocolos de camada superior; no modo túnel, os protocolos são empregados como um túnel de pacotes IP.

- **Protocolo IP.** No protocolo IP original, temos basicamente o cabeçalho IP, o TCP e os dados:

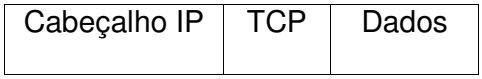

Figura 7.4: Protocolo IP original.

Protocolo IPSec – Modo Transporte. Nesta implementação o cabeçalho ESP é inserido entre o cabeçalho IP original e os demais componentes. Este modo deve ser utilizado na transmissão de dados entre hosts.

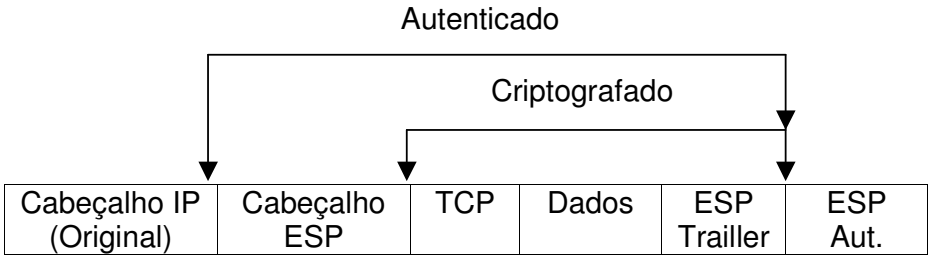

Figura 7.5: IPSec (modo transporte).

- **Protocolo IPSec – Modo Túnel.** Nesta implementação o cabeçalho IP Novo (externo) especifica o endereço do pacote de acordo com o modelo IPSec, enquanto o cabeçalho IP Original (interno) determina o endereço real do pacote IP. Este modo deve ser utilizado na transmissão de dados entre gateways.

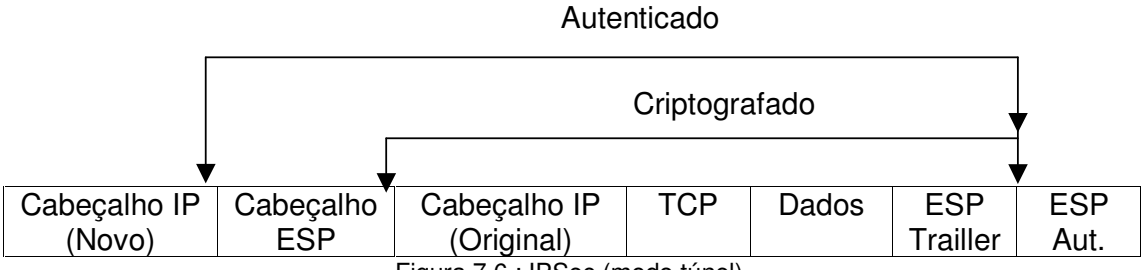

Figura 7.6 : IPSec (modo túnel).

7.4 – VPNs (Redes Privadas Virtuais).

O conceito de VPN [67] surgiu da necessidade de se utilizar uma rede pública, como a Internet, em vez de linhas privativas para implementar redes corporativas. O crescimento da estrutura da Internet, bem como a melhoria da qualidade das transmissões, tornou-a conveniente para as comunicações corporativas.

A utilização de redes públicas oferece uma redução de custos para as comunicações corporativas. Como exemplo pode-se citar o caso de uma empresa que tenha filiais em cidades diferentes e distantes, sendo que estas devem trocar informações através de seus computadores.

Na rede privada convencional, existe a necessidade que um computador esteja conectado a outro através de um link especificamente dedicado para a conexão. Esta situação se torna mais dispendiosa nos casos em que este link assume grandes distâncias, principalmente para links internacionais.

Através do uso de uma VPN, os dados trafegam via Internet, sendo necessário apenas uma discagem local para o provedor de acesso do computador.

O conceito de uma VPN mais extensa, através da Internet, é também denominado S/WAN (Secure Wide Area Network). Porém, o mais comum é que seja utilizado de forma genérica o termo VPN.

O problema de se utilizar a Internet é que os dados corporativos passam a trafegar num ambiente inseguro, como foi mostrado nos capítulos 3 e 5.

Sendo assim, para que este conceito se torne efetivo, uma VPN deve garantir:

- **Confidencialidade:** Os dados que trafegam na VPN não devem ser interceptados.

- **Integridade:** Mesmo que alguma transmissão seja interceptada, deve-se garantir que as informações transmitidas não possam ser alteradas.

- **Autenticidade:** Somente os usuários e os computadores pertencentes à VPN podem transmitir dados entre si. Um computador que faça parte da VPN somente reconhece as informações que forem geradas por outro computador que faça parte da VPN.

A segurança das informações também depende da forma como é implementada a VPN. São possíveis dois modos para esta implementação :

- **Modo Transporte:** Somente os dados são criptografados, sendo que o cabeçalho original do IP é mantido estando sujeito a análise do tráfego.

- **Modo Túnel:** Neste modo há um tunelamento entre os hosts, pois um novo IP é adicionado. Pode ser subdividido também em dois modos :

    - **Modo Túnel Criptografado:** Nesta implementação, os dados e o cabeçalho dos pacotes são criptografados.

    - **Modo Túnel não Criptografado:** Esta solução não implementa criptografia. Dados e cabeçalhos são transmitidos em sua forma

original, porém somente o novo endereço IP é atribuído. A falha desta solução é que os dados transmitidos não estão protegidos.

A criptografia das informações em uma VPN é realizada através dos conceitos de criptografia e autenticação que foram demonstrados no capítulo 6.

Quanto aos protocolos, os mais comuns são o IPSec, PPTP, L2TP e L2F.

Quanto às formas de aplicação, as mais comuns são:

7.4.1 – Acesso remoto via Internet.

Esta forma de aplicação ocorre quando um computador remoto se conecta à Internet através de um provedor de acesso. Através deste acesso remoto é estabelecido uma VPN, utilizando recursos de software, que permitem ao usuário remoto poder utilizar a rede corporativa de forma segura (figura 7.7).

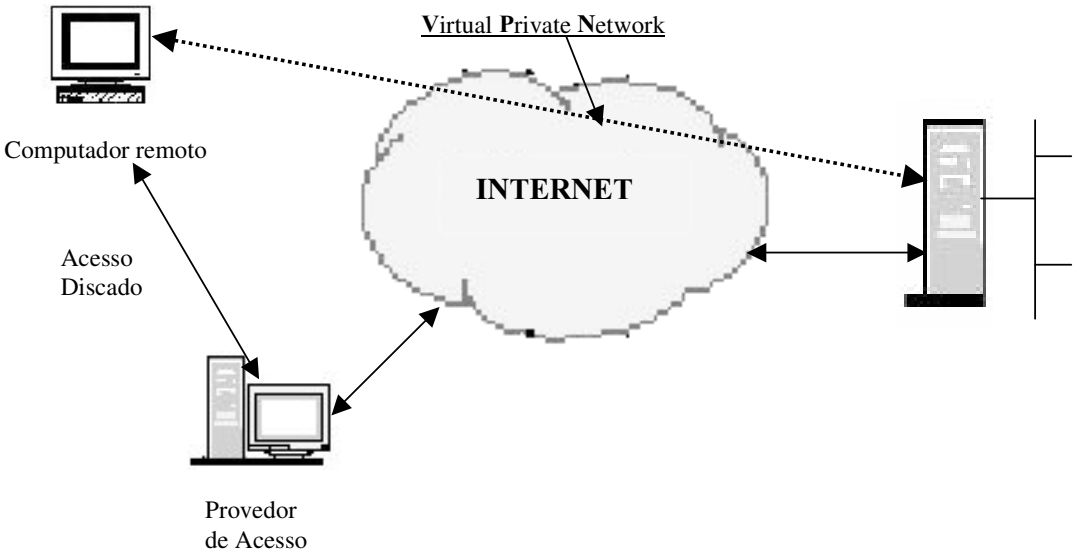

Figura 7.7: VPN com acesso remoto.

7.4.2 – Conexão de Lans via Internet.

Em empresas que mantém mais de uma planta, a comunicação entre as redes das diversas plantas (matriz e filial, filial 1 e filial 2, etc), muitas vezes tem que ser realizadas por linhas dedicadas de longa distância.

O conceito da VPN pode ser utilizado para permitir que esta conexão entre as diversas plantas possa ser implementada através da Internet. A comunicação segura entre as diversas plantas é estabelecida utilizando-se a estrutura da Internet.

Desta forma pode-se obter uma WAN (Wide area network) corporativa, sem a necessidade de possuir linhas privadas dedicadas à comunicação entre as diferentes redes da empresa (figura 7.8).

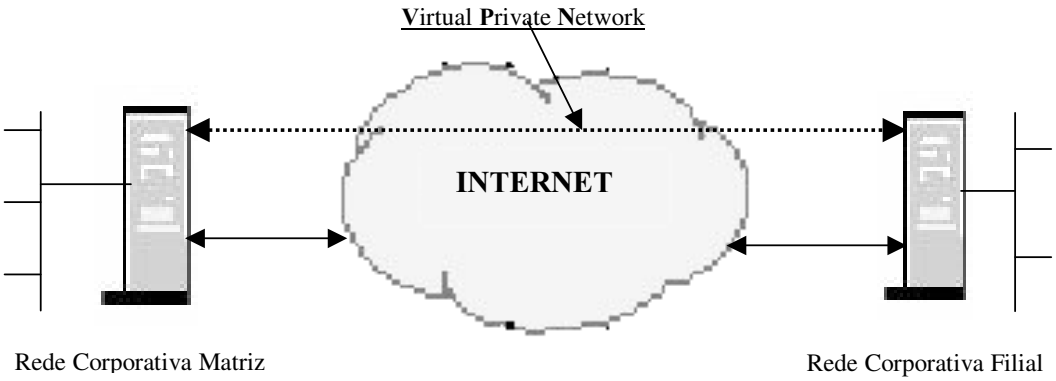

Figura 7.8: Conexão de Lans via Internet.

7.4.3 – VPN e Intranet.

O conceito de VPN também pode ser utilizado para garantir que um determinado grupo possa ter acesso à parte da rede não compartilhada por todos os usuários, por questão de segurança e restrição das informações disponíveis.

A solução mais comum para este problema é criar uma rede para este grupo de usuários separadamente da rede corporativa, de forma que os dados que circulem nesta rede departamental não estejam ao acesso dos demais usuários da rede corporativa.

A solução que envolve o conceito de VPN consiste em instalar um servidor VPN entre a rede corporativa e a rede local departamental.

Desta forma, apenas usuários habilitados pelo administrador do sistema poderão se comunicar com o servidor VPN e acessar as informações da rede departamental. Os demais usuários, não conseguirão sequer visualizar a existência da rede protegida (figura 7.9).

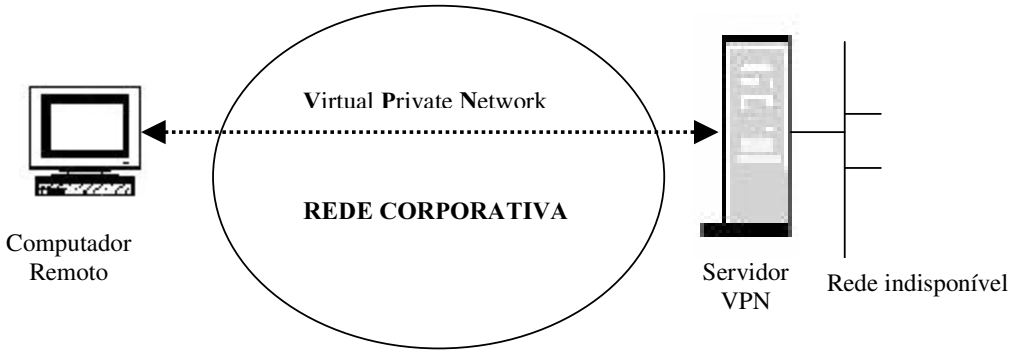

Figura 7.9: VPN interna à Lan.

7.5 – O protocolo SET.

O protocolo SET (Secure Electronic Transaction) [68] é um conjunto de especificações técnicas desenvolvidas por um grupo de trabalho liderado pela VISA e a Mastercard, com participação das empresas GTE, IBM, Microsoft, Netscape,

RSA, SAIC, Terisa e Verisign, com o objetivo de resolver os problemas de consumidores e comerciantes, que se utilizam de cartão de crédito para operações comerciais, através de redes abertas, de forma segura.

7.5.1 – Participantes do SET.

No protocolo SET os participantes do sistema são definidos da seguinte forma:

- **Cardholder** – É a pessoa que se utiliza do cartão de crédito. Que será também denominado como comprador.
- **Issuer** – É a instituição financeira que fornece o cartão de crédito para o Cardholder, garantindo o pagamento das transações devidamente autorizadas.
- **Merchant** – É o vendedor autorizado a aceitar cartões de crédito do Cardholder. Também denominado comerciante.
- **Acquirer** – É a instituição financeira que permite ao Merchant receber os valores transacionados.
- **Third partyes** – O Issuer e o Acquirer podem escolher uma entidade para processar as transações de pagamentos.
- **Payment gateway** – É um dispositivo operado pelo Acquirer ou um Third party, utilizado para o processamento dos dados relativos a autorizações de pagamentos.

7.5.2 – Etapas do SET.

A utilização do protocolo SET envolve as seguintes etapas:

1. O comprador (Cardholder), informa ao vendedor (Merchant) os produtos e o cartão de crédito que vai utilizar.

2. O comerciante após receber as informações, envia uma resposta ao comprador, contendo um identificador da transação, o certificado gerado pelo dispositivo (Payment gateway). Esta resposta contém a assinatura digital.

3. O comprador verifica a integridade e autenticidade dos dados enviados pelo comerciante e emite dois documentos eletrônicos:
    - Destinado ao comerciante, contendo:
        - Identificação do banco emitente do cartão;
        - Identificação do produto;
        - Identificação do local de entrega do produto.
    - Destinado ao Payment Gateway, contendo:
        - Número do cartão;
        - Validade do cartão;

Ambos os documentos devem estar relacionados pelo identificador da transação gerado pelo comerciante.

4 – O vendedor verifica a integridade e autenticidade das informações recebidas e envia ao Payment Gateway para o processar o pagamento.

Se o processo for autorizado o comerciante envia a fatura ao comprador.

7.5.3 – Conceitos do SET.

Os conceitos utilizados no protocolo SET são os mesmos já estudados anteriormente. A integridade e autenticação são garantidas pelo uso de assinaturas digitais, a partir da utilização de chaves públicas e privadas, message digest e certificados digitais.

Um dispositivo de segurança que deve ser citado é a assinatura dual. Esta assinatura digital é necessária quando duas mensagens diferentes, relacionadas entre si e que tem dois destinatários diferentes, devam ser confirmadas, porém, sem que um destinatário veja o conteúdo da mensagem endereçado ao outro.

Normalmente o comprador vai gerar duas informações distintas: A ordem de compra e a instrução de pagamento. Apesar de estarem relacionadas às informações tem destinatários diferentes.

Enquanto a ordem de compra interessa ao comerciante, pois contém os detalhes da encomenda, a instrução de pagamento contém os detalhes da transação, que interessam somente à instituição financeira (Acquirer).

O comprador gera dois hashes: um a partir da ordem de compra e outro a partir da instrução de pagamento.

Após a concatenação destes dois hashes é gerado um novo hash, que deverá ser assinado, com a chave privada do comprador, criando assim a assinatura dual, conforme figura 7.10:

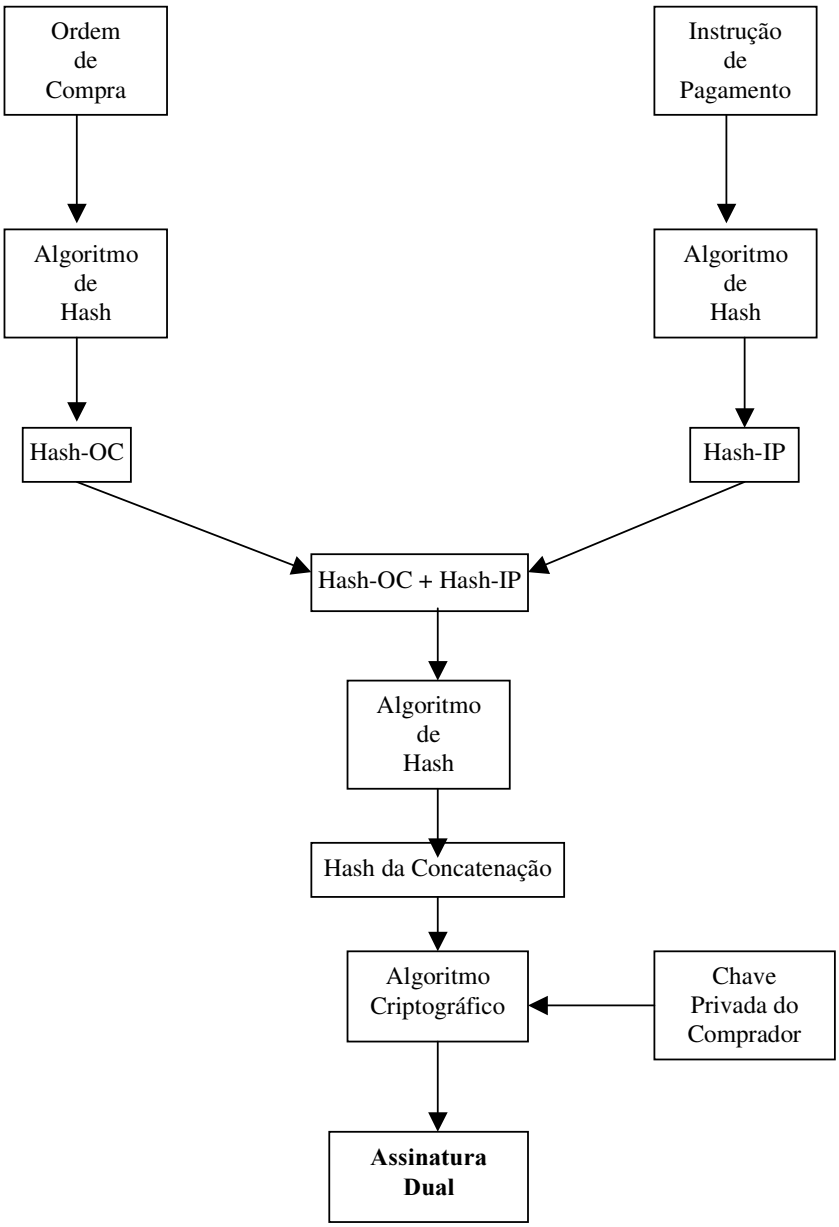

Figura 7.10: O esquema da assinatura dual.

A conferência da integridade das informações, por parte do comerciante acontecerá a partir das informações enviadas pelo comprador:

- Ordem de Compra;

- Assinatura Dual;
- Hash-IP (da Instrução de Pagamento);
- Chave publica do comprador, devidamente garantida pelo certificado digital.

De posse destas informações o comerciante faz a conferência em três etapas distintas e complementares:

1. O comerciante aplica o algoritmo de hash sobre a Ordem de Compra para obter o Hash-OC, concatenando-o ao Hash-IP.
2. Num segundo instante, o comerciante utiliza a chave pública para decriptografar a assinatura dual e obter os hashes concatenados, que foram gerados pelo comprador.
3. Finalmente basta ao comerciante, comparar a concatenação que ele calculou, com a concatenação que ele decriptografou do comprador.

   Se as duas concatenações forem iguais, o comerciante constata assinatura do comprador e também a integridade da Ordem de Compra.

No caso, a Instrução de Pagamento serviu para esta verificação, porém, em nenhum momento esteve acessível para o comerciante, pois o comerciante apenas teve posse do hash da Instrução de Pagamento (Hash-IP), sem ter o texto original da instrução de pagamento.

Como a partir do hash é impossível obter o texto original (Cap. 6, item 4), a instrução de pagamento estará inacessível para o comerciante.

A situação pode ser ilustrada como na figura 7.11:

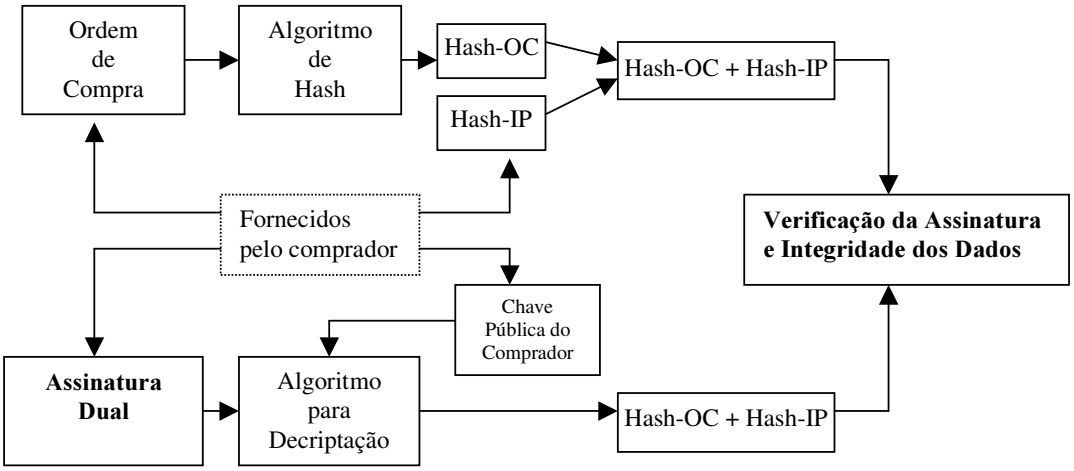

Figura 7.11: A conferência da assinatura digital pelo comerciante.

De forma similar, a instituição financeira que receber a assinatura dual, poderá confirmá-la sem ter acesso à Ordem de Compra, conforme a figura 7.12:

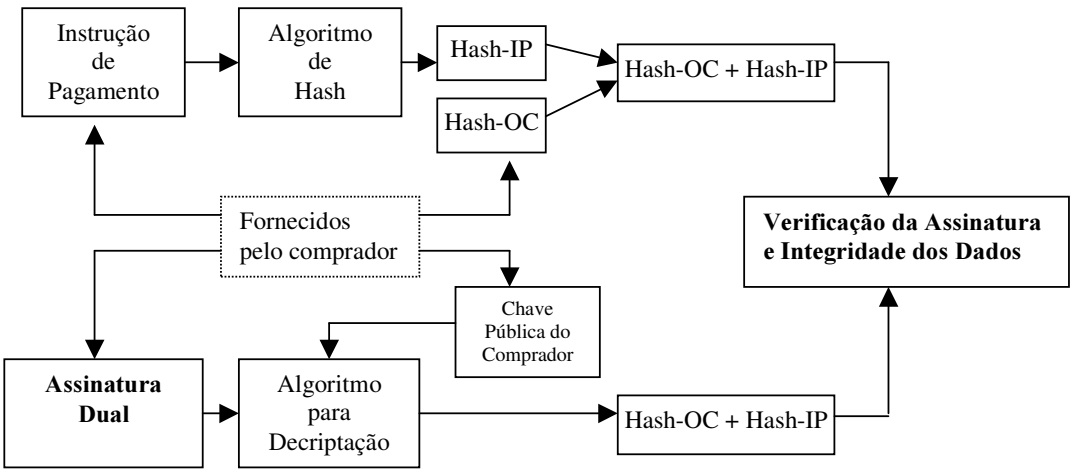

Figura 7.12: A conferência da assinatura digital pela instituição financeira.

7.6 – Outros Mecanismos.

Existem diversos mecanismos de pagamento para possibilitar o comércio eletrônico, os quais se originaram no EDI e no EFT. Entre os principais meios podemos citar:

7.6.1 – CyberCash.

O CyberCash [69] é um sistema concebido por William Melton em 1994, que pertencia a empresa de mesmo nome (Cybercash) e que foi adquirida pela Verisign.

O objetivo do Cybercash é assegurar o pagamento eletrônico através do uso do cartão de crédito na Internet.

O CyberCash funciona basicamente através do uso de três entidades diferentes [70] :

- Consumidor – Que deve portar o software do consumidor (Wallet)
- Comerciante – Que deve portar uma aplicação Server
- CyberCash – Que também deve ter uma aplicação Server.

Os processos de compra, transação e pagamento ocorrem da seguinte forma:

- O consumidor escolhe os produtos e notifica o comerciante;
- O comerciante apresenta o valor da compra e solicita o formulário de pagamento.
- O consumidor envia o formulário de pagamento codificado ao comerciante.

- As três entidades envolvidas trocam mensagens cifradas através da Internet e das redes das empresas de cartões de crédito, ligadas à CyberCash.

A CyberCash fatura, cobrando uma taxa sobre as operações que processa.

7.6.2 – First Virtual.

O sistema First Virtual Holdings [71], também foi desenvolvido para permitir o pagamento com cartão de crédito através da Internet.

Para que o First Virtual possa ser utilizado é necessário um cadastro prévio do comprador junto à First Virtual. O cliente fornece informações pessoais e financeiras e recebe um código denominado Virtual Pin.

Os processos de compra, transação e pagamento ocorrem da seguinte forma:

- O consumidor escolhe os produtos, notifica o comerciante e fornece o seu Virtual Pin.
- O comerciante envia os dados da compra e o Virtual Pin do consumidor à First Virtual.
- A First Virtual verifica se o comprador está devidamente autorizado e envia uma mensagem eletrônica (correio eletrônico) para o comprador, que terá três possibilidades de resposta:
    1. Concordando em pagar;
    2. Discordando dos dados fornecidos pelo comerciante;
    3. Notificando à First Virtual, que não reconhece a compra.

Se a resposta dada pelo comprador for a primeira opção, o comerciante receberá a autorização para concluir a negociação. Porém o pagamento somente será efetuado (débito na conta do cliente e repasse para o comerciante), quando o comprador acusar o recebimento da encomenda.

O cliente que não efetuar devidamente o pagamento, terá seu Virtual Pin suspenso.

7.6.3 – NetCheque.

O NetCheque [72] é um sistema baseado no uso de cheques eletrônicos.

Um cheque eletrônico é uma versão eletrônica dos cheques tradicionalmente utilizados, para que este possa ser utilizado na Internet.

O cheque eletrônico utiliza uma entidade denominada Third-party Account Server para verificação e processamento dos valores transacionados.

O sistema do NetCheque funciona da seguinte forma [73]:

- O comprador efetua suas compras e escolhe seus produtos;
- O comprador envia o cheque eletrônico para o vendedor como forma de pagamento;
- O comerciante recebe o cheque eletrônico e envia-o ao account server, para verificação e pagamento;
- O account server confirma os dados do comprador através da sua assinatura digital, enviando a confirmação ao vendedor;
- A assinatura digital é a base para que o banco transfira o valor para a conta do comerciante.

Caso algum comprador emita um cheque eletrônico sem ter o devido saldo em conta, será desligado da NetCheque.

7.6.4 – Echeck.

O Echeck [74] também é uma modalidade de cheque eletrônico. É um pouco mais amplo do que o NetCheque, pois permite a utilização de cartões de débito e transferência de valores.

Para usar o Echeck, o cliente deve se cadastrar em uma empresa que utilize o sistema. Uma vez que o cliente esteja cadastrado, a instituição fornece ao cliente uma forma de possuir a sua chave secreta e chaves simétricas. Isto pode ser feito através da instalação de um software junto ao cliente, ou fornecimento de um cartão (Smartcard ou PCMCIA).

Através de um software que implementa integridade e confidencialidade dos dados, o Echeck providencia a transferência dos fundos para possibilitar o pagamento do comerciante nos mesmos moldes do NetCheque.

7.6.5 – eCash.

O eCash é uma modalidade de pagamento conhecida como dinheiro eletrônico.

O dinheiro eletrônico é definido através de 4 propriedades, segundo Kalakota [16]:

1. **Valor monetário**. O dinheiro eletrônico deverá ser convertido em dinheiro, ou crédito.
2. **Interoperabilidade**. O dinheiro eletrônico pode ser trocado por mercadorias em diversos lugares.

3. **Ser armazenável e recuperável**. O dinheiro eletrônico deve ter a capacidade de ser armazenado e de poder ser recuperado.
4. **Ter segurança**. O dinheiro eletrônico deve ter os conceitos de integridade e confidencialidade.

Para utilizar a “moeda digital” [75] o usuário do ecash, deve obtê-las via Internet de um banco participante do sistema ecash, do qual o usuário seja correntista. Quando for efetuar um pagamento, junto a um comerciante que aceite o ecash, basta transferir o valor correspondente para o comerciante.

O sistema pode ser explicitado da seguinte forma:

- **Obtenção da moeda digital:** o usuário utiliza o software cyberwallet para gerar a quantidade de moedas digitais desejadas. O software atribui a cada moeda um número de identificação aleatório. As moedas são criptografadas com a chave pública do banco, assinada digitalmente pelo usuário e enviadas ao banco. O banco retira o valor correspondente da conta do usuário, assina as moedas com sua chave privada e as envia criptografadas com a chave pública do usuário.

- **Utilização da moeda digital:** para fazer um pagamento com a moeda digital o usuário deve enviá-las para o comerciante criptografadas com a chave pública do comerciante. O comerciante deve possuir a chave pública do banco para confirmar a autenticidade das moedas digitais, a partir da assinatura digital do banco.

- **Transformação em moeda real:** a moeda digital é convertida em dinheiro real, quando o comerciante as envia para o banco. Neste momento as moedas digitais são registradas como utilizadas pelo banco e o valor correspondente em moeda real é depositado na conta do comerciante.

7.6.6 – Smart Cards.

Um Smart Card [76] é um cartão de plástico, semelhante a um cartão de crédito, o qual possui um microchip embutido. Este microchip pode ter diversas utilidades que permitem atribuir as seguintes classificações aos Smart cards:

- **Memory card**. É uma versão mais simples do Smart card, que possui apenas a capacidade de armazenar informações, necessitando de leitores específicos para recuperá-las. Normalmente este tipo de cartão é utilizado apenas para efetuar pagamentos.
- **Shared-key card**. Este tipo de Smart card possui a capacidade de processamento no próprio microchip. Nesta modalidade chaves secretas são incluídas no microchip, além de software com o algoritmo criptográfico, permitindo assim a autenticação do cartão.
- **Signature-transporting card**. Semelhante ao shared-key card, porém com um algoritmo criptográfico diferenciado.
- **Signature-creating card**. Nesta modalidade o microchip possui a capacidade de gerar assinaturas digitais.

De forma geral, os Smart cards são utilizados para armazenar informações que podem ser pessoais, financeiras ou preferenciais, possibilitando o pagamento de contas, ou servindo como uma alternativa de substituição ao dinheiro tradicional.

Apesar da semelhança com o cartão de crédito, o Smart card apresenta as seguintes vantagens:

1. É mais indicado para transações eletrônicas, devido aos mecanismos de segurança que apresenta.
2. Possui uma maior capacidade de armazenamento de dados;
3. Apresenta um maior potencial de aplicações, pois possibilita o processamento de informações.

Uma das formas mais avançadas de utilizar o Smart card pode ser exemplificada através do sistema Mondex [77], que é um dos sistemas pioneiros na utilização de Smart card como dinheiro eletrônico. Neste sistema um cartão carregado no banco pode ser utilizado pelo proprietário do cartão para diversas funções, como até mesmo, creditar um determinado valor para o Smart card de outra pessoa.

CAPÍTULO 8

O uso do protocolo HTTPS como ferramenta de segurança na transmissão de dados

---

Este capítulo apresenta, o funcionamento do protocolo seguro HTTPS. A análise do funcionamento deste protocolo merece destaque nesta dissertação, pelo fato deste ser um dos protocolos mais utilizados pelos sites Internet Banking e de comércio eletrônico de um modo geral.

8.1 – HTTPS.

O HTTPS é uma aplicação que tem por finalidade garantir segurança nas transmissões de dados através da Internet, em aplicações como Home Banking, compras por cartão de crédito, e-commerce, enfim, aplicações comerciais que envolvam valores, informações privadas, senhas, etc.

O HTTPS é a utilização do protocolo HTTP (HyperText Transfer Protocol) em conjunto com o protocolo SSL (Secure Sockets Layer), que é um protocolo proposto pela Netscape Communications com apoio da Verisign e da Sun, e foi lançado inicialmente em 1994.

O SSL foi desenvolvido e especificado para implementar uma camada de segurança entre a camada de transporte (TCP) e os protocolos de aplicação, tais como HTTP, TELNET, FTP, etc; tendo se tornado praticamente um padrão para as aplicações de e-commerce.

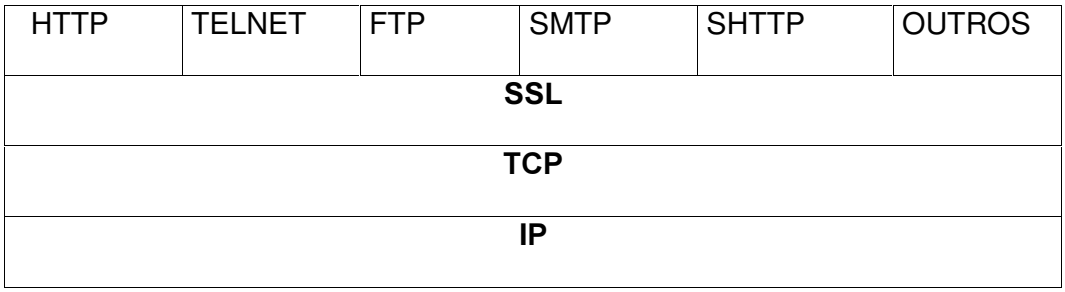

Figura 8.1: A camada SSL.

A camada SSL, na arquitetura TCP/IP, fica entre a camada de transporte IP e a camada de aplicação, constituindo-se assim em uma camada de sessão que torna segura a transação cliente-servidor.

O HTTPS pode ser considerado, sob o ponto de vista do browser, como um protocolo único, obtido pela associação dos protocolos HTTP e SSL, sendo assim necessário utilizar "https://" para URLs HTTP com SSL, enquanto que a URL "http://" continua sendo utilizada para páginas HTTP sem SSL.

A porta default para o https é a porta número 443, definida pela IANA. [78]

Os dados trocados entre o servidor e o browser são criptografados. Desta forma, o HTTPS pode ser utilizado para transações seguras na Internet.

Um ícone (que pode ser uma chave ou um cadeado) indica também se o documento foi criptografado ou não. Se o ícone mostra o desenho de uma chave ou cadeado rompido, significa que não houve criptografia do documento. Caso contrário, a chave ou cadeado aparecem intactos.

8.2 – Condições para uso do HTTPS.

Para a transação segura ocorrer, o HTTPS deve estar ativado no servidor e pode estar ativado no cliente. Isto é, não é necessário o cliente ter https ativado, porém, o cliente deve ter um browser habilitado para o protocolo SSL.

As últimas versões dos browsers encontrados no mercado são habilitados para o protocolo SSL. Caso o cliente não possua um desses browsers, ele ainda pode fazer comunicação segura através de um proxy que seja habilitado. Entretanto, dessa maneira, a conexão segura ficará restrita à conexão entre o proxy e o servidor.

O cliente dificilmente deverá digitar uma URL usando HTTPS, pois normalmente ele estará em uma página HTTP e apenas iniciará uma conexão segura através de um link para a página que utiliza o protocolo HTTPS. Por exemplo, para entrar na página segura de uma determinada empresa, o cliente inicia a navegação através da página corporativa da empresa. Para isto terá que digitar o protocolo padrão, com a URL iniciada por “http://”.

Após isso, escolherá os artigos que quer comprar, ou a transação que deseja realizar e apenas quando clicar no ícone que finaliza a compra ou a transação, no momento que as informações sigilosas deverão ser digitadas (conta, senha, número do cartão de crédito, etc), ele entrará em uma conexão segura que utilizará o HTTPS.

Neste momento, quando a conexão segura é iniciada, o browser deve apresentar o ícone especial (cadeado), por onde se pode verificar informações da certificação digital.

8.3 – Certificação.

Um ponto importante no HTTPS é o uso de certificados digitais. Para o HTTPS ser ativado deve-se possuir um certificado. Logo, como todo servidor deve ter https ativado, ele deve ser certificado.

Receber um certificado digital é a garantia para o cliente de que ele está mandando os dados para o host correto. Isso é, o servidor é exatamente quem ele diz ser.

O cliente pode conseguir informações do certificado do servidor através do browser, clicando no ícone em formato de cadeado.

8.4 – Protocolo SSL.

O protocolo SSL [79] é aberto e tornou-se um padrão de segurança para browsers e servidores na World Wide Web. Sua especificação está proposta em documento publicado pela Netscape [80] e baseado em sua proposta surgiu também o protocolo TLS (Transaction Layer Security) [81].

O objetivo principal do protocolo SSL é implementar privacidade e confiabilidade entre dois programas aplicativos que se comunicam. Seu projeto leva em conta a existência de diversos programas de aplicação e diversas plataformas com diferentes sistemas operacionais e busca estabelecer um processo de negociação e emprego de funções de autenticação mútua, criptografia de dados e integridade para transações seguras entre aplicações na Internet, da forma mais simples e transparente possível.

O SSL consiste de uma criptografia simétrica aninhada dentro de uma criptografia de chave assimétrica, autenticada através do uso de certificados. Uma conexão SSL só pode ocorrer entre um cliente SSL-enabled e um servidor SSL-enabled.

O SSL negocia um algoritmo de criptografia, uma chave de sessão e autentica o servidor antes de qualquer transmissão.

O protocolo SSL tem três propriedades básicas:

- A identidade do cliente e do servidor pode ser autenticada usando algoritmo de criptografia com chave assimétrica (ou pública), tal como RSA ou DSS.
- A conexão é privada. O mecanismo de criptografia é utilizado depois de uma negociação inicial, o (handshake - aperto de mão), com a finalidade de definir uma chave secreta. Após o handshake é utilizada a criptografia simétrica para criptografar os dados, tal como DES ou RC4.
- A conexão é confiável. O transporte de mensagens inclui um mecanismo de checagem da integridade da mensagem usando MAC (Message Authentication Code) com as funções de hash SHA ou MD5.

No processo de autenticação mútua é estabelecida a confiança entre cliente e servidor por mecanismos de identificação.

A criptografia dos dados, por sua vez, adiciona privacidade e confidencialidade na comunicação pela aplicação de diversos algoritmos que podem ser suportados pelo protocolo, conforme as necessidades da aplicação. Também garante a integridade dos dados, assegurando que estes não sejam adulterados intencionalmente ou acidentalmente.

Desta forma, o protocolo SSL implementa criptografia dos dados, autenticação de servidor, integridade de mensagem e, opcionalmente, autenticação de cliente para uma conexão TCP/IP.

Uma das vantagens do protocolo SSL é o fato de ser um protocolo independente da aplicação. Um protocolo de alto nível pode ser suportado sobre o SSL de forma transparente. Os principais objetivos do protocolo SSL, em ordem de prioridade, são:

- **Segurança criptográfica:** O SSL deve ser usado para estabelecer uma conexão segura entre um cliente e um servidor.

- **Interoperabilidade:** Programadores independentes devem ser capazes de desenvolver aplicações, utilizando SSL, que possam trocar parâmetros com sucesso entre si sem conhecerem os códigos uma da outra.

- **Extensibilidade:** O SSL mantém uma estrutura na qual novas chaves públicas e métodos de criptografia possam ser incorporados, sem a necessidade de desenvolver novos protocolos.

- **Eficiência:** Operações de criptografia costumam ter processamentos pesados, particularmente em operações com algoritmos de chave pública. Durante a negociação inicial (handshake) esta estratégica criptográfica é utilizada pelo SSL gerando um overhead. Por esta razão, o protocolo SSL incorpora um sistema de cache para reduzir o tempo de processamento. Este sistema armazena as informações negociadas durante o handshake

e no caso de uma nova conexão num curto espaço de tempo, estas informações (chave secreta, estratégia criptográfica, etc) serão recuperadas e reutilizadas, representando um ganho de tempo significativo.

8.5 – Composição do Protocolo SSL.

O Protocolo SSL é um protocolo estruturado em camadas. Em cada camada as mensagens podem incluir campos para determinar o tamanho, a descrição e o conteúdo da mensagem.

O protocolo toma as mensagens a serem transmitidas pelas camadas superiores, fragmenta os dados em blocos, opcionalmente executa a compressão destes dados, aplica um MAC (Message Authentication Code), criptografa e finalmente transmite as informações processadas.

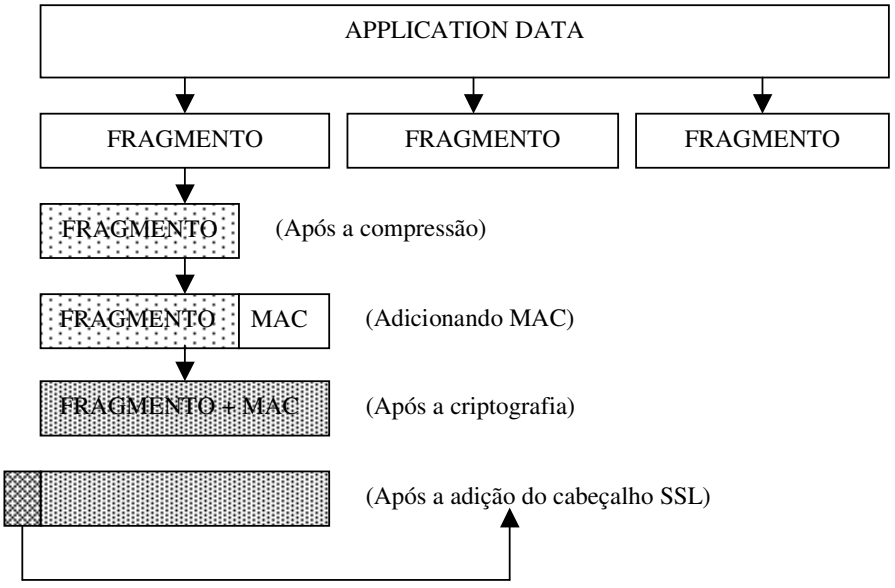

Figura 8.2: O protocolo SSL.

Os dados recebidos são decriptografados, verificados, descomprimidos e remontados, para então serem entregues aos clientes de camadas de nível superior

O protocolo SSL é composto de duas camadas, que podem ser designadas como nível inferior e nível superior, conforme a figura 8.3:

SSL	Nível Superior (Message Layer)	Handshake Protocol, Change Cipher Spec Protocol, Alert Protocol e Application Data Protocol.
	Nível Inferior (Record Layer)	

Figura 8.3 – Camadas do SSL.

8.5.1 – Nível Inferior.

O nível inferior (Record Layer) é suportado por um protocolo de transporte, como, por exemplo, o TCP. O nível inferior é utilizado para encapsular os diversos protocolos de nível superior e implementar os serviços de fragmentação, compressão, autenticação de mensagem e criptografia.

Na fragmentação, os blocos de informação são quebrados em registros SSL Plaintext de até 224 bytes.

Na compressão, os registros SSL Plaintext são transformados em um registro SSL Compressed. Na descompressão ocorre exatamente o processo inverso. Para isto é utilizado o algoritmo de compressão e descompressão negociado no estado de sessão.

8.5.2 – Nível Superior.

No nível superior (Message Layer) além do protocolo de aplicação, são inseridos protocolos auxiliares para implementar os recursos de segurança :

- **SSL Handshake Protocol:** Permite ao servidor e ao cliente autenticarem-se mutuamente, negociarem um algoritmo de criptografia e as chaves criptográficas, antes do protocolo de aplicação transmitir ou receber os primeiros dados.

- **Change Cipher Spec Protocol:** Serve para negociar transições nas estratégias de criptografia. Consiste de uma única mensagem que é criptografada sob a especificação corrente de criptografia.

  Pode ser transmitida pelo cliente e pelo servidor para notificar à outra parte que o registro subseqüente será protegido por chaves de criptografia recém negociadas.

- **Alert Protocol:** Supervisiona erros na camada do SSL Record Protocol e possibilita a troca de mensagens de alerta para sinalizar erros de seqüência de mensagens, erros de certificação e de criptografia. Estes erros podem ser divididos em duas categorias:
  - Warning : um simples aviso de erro.
  - Fatal : um problema grave, que sinaliza o encerramento imediato da sessão.

- **Aplication Protocol:** Especifica que as mensagens de dados das aplicações sejam transportadas pela Record Layer e sejam fragmentadas, comprimidas e criptografadas com base no estado de conexão corrente. As mensagens são tratadas como dados transparentes pela Record Layer.

Dentre estes protocolos, o mais interessante é o SSL Handshake Protocol, pois é nele que os parâmetros criptográficos do estado da sessão são produzidos, sendo operado no topo da Record Layer.

Quando um cliente e um servidor SSL iniciam uma comunicação, eles inicialmente entram em acordo sobre uma versão de protocolo, selecionam algoritmos criptográficos, autenticam-se mutuamente (opcionalmente) e usam técnicas de chaves públicas de criptografia para gerar segredos comuns.

Todas as mensagens de handshake são trocadas usando MAC (Message Authentication Code) para dar segurança à transação desde o início do processo.

A ordem das mensagens obedece a uma seqüência absoluta, e as mensagens de negociação são criadas nesta camada e manuseadas pela Record Layer.

O handshake do SSL acontece em duas fases distintas. A primeira fase é utilizada para estabelecimento de uma conexão privada de comunicação, enquanto que a segunda realiza a autenticação do cliente.

O handshake pode ser melhor especificado através da tabela 8.1 :

CLIENTE	SERVIDOR
1 – Envia a mensagem “Client Hello”.	
	2 – Resposta com um “Server Hello”.
	3 – Envia o “Server Certificate”.
	4 – Envio (opcional) do “Server Key Exchange”
	5 – Envio (opcional) do “Certificate Request”.
	6 – Envia a mensagem “Server Hello Done”
7 – Envia o “Certificate Message” ou “No Certificate”.	
8 – Envia a mensagem “Client Key Exchange”.	
9 – Envia o “Certificate Verify”.	
10 – Envia a mensagem “Change Cipher Spec”.	
11 – Envia a mensagem “Client Finished”.	
	12 – Envia o seu “Change Cipher Spec”.
	13 – Envia a mensagem “Server Finished”.

Tabela 8.1: O handshake protocol.

Detalhando a seqüência descrita a partir de cada passo numerado, temos :

Detalhando a seqüência descrita a partir de cada passo numerado, temos :

1 e 2 – A mensagem Client Hello é utilizada para um cliente contatar um servidor. As mensagens Client Hello e Server Hello, estabelecem os seguintes atributos: Versão de protocolo, identificação de sessão, conjunto de criptografia e método de compressão. Adicionalmente, dois valores numéricos e aleatórios (ClientHello Random e ServerHello Random) são gerados e trocados entre cliente e servidor. No conjunto criptográfico são estabelecidos:

- Um algoritmo assimétrico para troca de chaves;
- Um algoritmo para criptografar os dados;
- Um algoritmo para adicionar uma redundância nas mensagens.

3 – Para que o servidor possa ser autenticado ele deverá enviar o seu certificado digital.

4 – Caso seja necessário, o servidor deverá enviar o “Server Key Exchange”. Isto somente deverá ocorrer se o servidor não possuir um certificado, porém, neste caso o cliente receberá um alerta, decidindo se deve prosseguir ou não.

5 – Opcionalmente, o servidor pode requisitar que o cliente possua um certificado. Este passo somente ocorrerá caso o servidor queira autenticar o cliente.

6 – O servidor envia a mensagem “Server Hello Done”, indicando que a fase inicial do handshake (Hello) está completada.

7 – Se o servidor enviou o “Certificate Request” solicitando um certificado por parte do cliente, ele deverá enviar seu certificado digital, através da “Certificate Message” ou, caso não possua um certificado, enviar a mensagem “No Certificate”.

8 – O “Client Key Exchange” será enviado. Seu conteúdo é baseado no algoritmo de criptografia pública negociado nos passos 1 e 2, pois a partir daqui as mensagens são criptografadas com base no mesmo.

9 – Este passo somente acontecerá caso o cliente tenha enviado seu certificado digital. O “Certificate Verify” possibilita que o certificado seja confirmado.

10 – O “Change Cipher Spec” contém as especificações para que se possa fazer os últimos ajustes no conjunto criptográfico.

11 – A mensagem “Finished” serve para encerrar o handshake por parte do cliente. Esta mensagem contém o novo algoritmo simétrico e a respectiva chave secreta a ser utilizada.

12 – O servidor envia o seu “Change Cipher Spec”, ajustando as suas especificações criptográficas.

13 – O servidor envia uma mensagem de “Finished”, já com as especificações criptográficas, finalizando todo o processo de handshake. A partir deste passo a criptografia passa a ser simétrica e o SSL passará a tratar efetivamente a aplicação.

Uma vez que o handshake tenha sido completado, as duas partes trocam chaves secretas, que serão usadas para criptografar os registros e computar códigos de autenticação de mensagens (MAC) sobre seus conteúdos. As técnicas utilizadas na criptografia e na função MAC são definidas na mensagem Cipher Spec.

Estas funções transformam um texto SSL Compressed em um texto SSL Ciphertext. A transmissão inclui também um número de seqüência para detectar perda de mensagens ou mensagens alteradas.

O algoritmo MAC é computado antes da criptografia. Portanto o processo criptográfico é feito no bloco inteiro, incluindo o MAC.

8.6 - SSL Tunneling.

Quando é feita uma requisição SSL para um servidor seguro através de um proxy, quem abre a conexão com o servidor é o proxy, que apenas copia os dados

em ambas as direções, lembrando que a presença do proxy não acarreta perda de segurança, desde que o cliente também esteja habilitado para o protocolo SSL.

Essa emulação de um túnel através do proxy [82] é chamada de "tunneling", e está esquematizada na figura 8.4.:

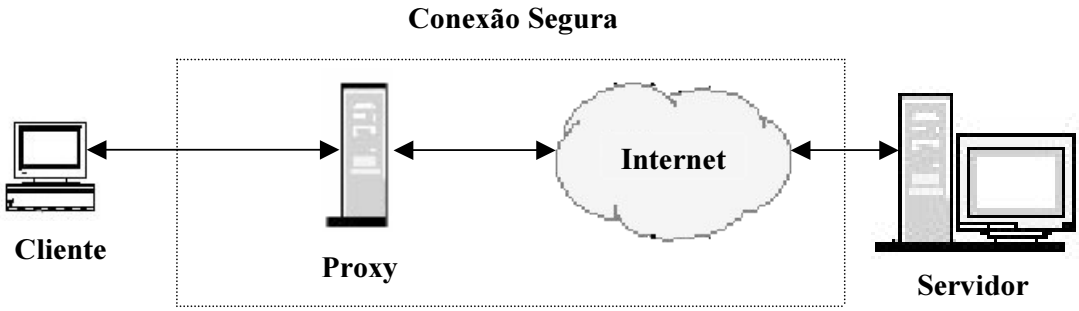

Figura 8.4: SSL tunelado.

Conforme visto anteriormente, para utilizar SSL tunneling, o cliente deve também suportar o protocolo SSL. Caso contrário, ele só poderá fazer conexão segura através de um proxy. Porém neste caso, a conexão será segura somente entre o proxy e o servidor.

A conexão entre o cliente e o proxy não será segura. Esta situação é ilustrada na figura 8.5.

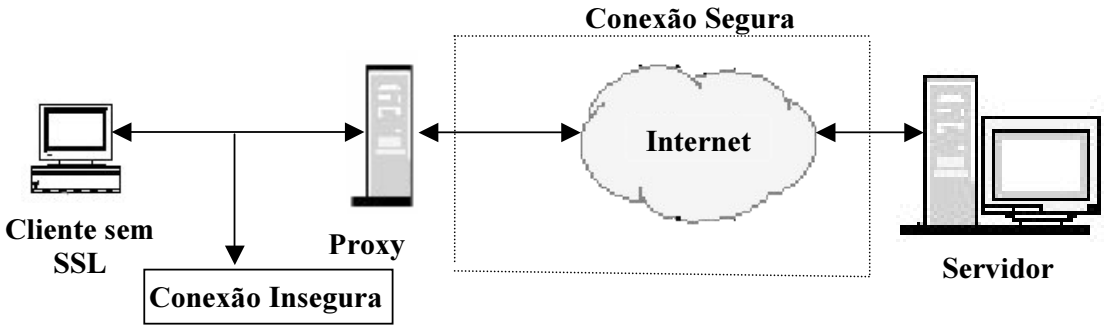

Figura 8.5: Conexão sem SSL no cliente.

8.7 – Resumo: Protocolo HTTPS e SSL.

- Um usuário, através de um browser, acessa o site do servidor que disponibiliza uma página segura (HTTPS). Esta conexão somente será possível se o usuário estiver com a opção de SSL ativada, ou através de um proxy com SSL ativado. Caso contrário, a página estará indisponível para este usuário.

- O servidor responde enviando seu certificado digital, autenticando-se. Caso o servidor não possua um certificado digital, uma mensagem de advertência é exibida ao usuário.

- O browser do usuário gera uma chave de sessão para criptografar todas as comunicações com o servidor.

- O browser do usuário criptografa a chave de sessão com a chave pública do servidor. O servidor então será o único a poder decriptografar os dados, e obter a chave de sessão.

- Uma sessão segura é estabelecida. Tudo acontece em segundos e não requer nenhuma ação do usuário. Um ícone no formato de uma chave ou de um cadeado é exibido, possibilitando ao usuário cliente ser notificado que a conexão segura foi estabelecida.

CAPÍTULO 9

Hospedagem segura

Este capítulo mostra uma opção de segurança para empresas que desejam implementar um site de comércio eletrônico seguro e que por questões que variam, desde a falta de corpo técnico especializado até a falta de recursos financeiros, não apresentam condições para implementar nenhuma das ferramentas de segurança apresentadas nos capítulos anteriores.

9.1 – Hospedagem.

Como já foi demonstrado no capítulo 2 o comércio eletrônico apresenta-se como um promissor mercado para as empresas. Porém, para que uma empresa entre para o mundo virtual, uma série de mecanismos são necessários.

Até aqui, destacamos apenas estes mecanismos de segurança (capítulos 7 e 8). No entanto, para que uma empresa possa aderir ao comércio eletrônico, uma série de outros requisitos são também exigidos: alta disponibilidade de hardware, banda larga para comunicações, roteadores, segurança física, nobreaks, além da capacidade de manter o serviço disponível 24 horas por dia, todos os dias do ano.

É lógico que nem todas as empresas que desejam entrar no mundo do comércio eletrônico podem dispor de todos estes recursos.

Neste vácuo existente entre o desejo da empresa aderir ao comércio eletrônico e a falta de infra-estrutura necessária para viabilizar esta adesão, surgiram as empresas de hospedagem.

As empresas que oferecem o serviço de hosting (hospedagem) são genericamente denominadas IDCs (Internet Data Center). Estas empresas são especializadas em manter uma infra-estrutura de informática voltada para hospedar sites de outras empresas.

Em Foresti [83] podemos encontrar a seguinte definição para IDC: *"Pode-se dizer que a denominação ´Internet Data Center´ tem implicações relativas à localização onde os sistemas de missão crítica para Web são mantidos"*.

9.2 – Infra-estrutura necessária para hospedagem.

Para que uma empresa de hospedagem possa dispor de uma infra-estrutura adequada, os seguintes requisitos devem ser atendidos:

- **Segurança física e lógica:** Neste tópico podemos considerar a segurança dos dados e a segurança física das instalações. Isto implica em dispor de acesso controlado ao interior da empresa, uso de câmeras de vigilância, segurança biométrica, etc.

- **Sistema de controle de incêndio:** Este é um item que está ligado à segurança física e que merece destaque. A empresa deve manter dispositivos que impeçam a progressão de um incêndio. Um dos meios mais difundidos na atualidade é o sistema que utiliza o gás FM-200 [84].

- **Comunicação de dados:** As comunicações devem estar disponíveis 24 horas por dia, todos os dias da semana. Desta forma, a capacidade de transmissão de dados deve ser estabelecida pelo pico de tráfego, a fim de manter ininterrupto o acesso ao site hospedado.

- **Disponibilidade de energia constante:** A empresa de hospedagem deve manter estabilizadores, baterias ou geradores, suficientes para o funcionamento do IDC, mesmo em caso de queda da energia elétrica.

- **Temperatura e umidade controladas:** Estes itens devem ser controlados a fim de garantir que os equipamentos disponibilizados possam trabalhar nos níveis de umidade e temperatura previstos.

- **Infra-estrutura física:** O ambiente onde os equipamentos do Data Center ficam instalados deve dispor de área suficiente para que estes possam funcionar em perfeitas condições.

- **Localização:** A localização das centrais do IDC determina os tipos de clientes que ele pode ter. Clientes que desejam disponibilizar seus sites mundialmente, necessitam que o IDC tenha sua central espelhada globalmente.

Concluindo, pode-se dizer que a infra-estrutura do IDC deve estar apta a oferecer o serviço de hospedagem com todos os requisitos necessários, primando pela segurança das instalações e estando preparado para enfrentar situações críticas, como: falta de energia, picos de comunicação, ou incêndios.

9.3 – Tipos de hospedagem.

Existem diversos pacotes de serviços de hospedagem oferecidos no mercado de IDCs. Esta diversificação de produtos pode ser definida através da seguinte relação: serviço oferecido X necessidade do cliente.

A existência de diferentes necessidades por parte dos clientes leva alguns IDCs a disponibilizarem “pacotes de produtos”. Estes pacotes de produtos vão desde uma simples hospedagem do site (desde que respeitados os requisitos vistos no item 9.2), até pacotes que disponibilizam produtos específicos para o comércio eletrônico, entre os quais pode-se citar: certificação digital, protocolo SSL, protocolo SET, etc.

Os últimos produtos mencionados constituem o que se pode conceituar como hospedagem segura.

9.4 – Hospedagem segura.

O conceito de hospedagem segura consiste num conjunto de serviços prestados por parte da empresa de hospedagem, que abriga as informações de seus clientes, cujo foco principal é a segurança da informação [85].

Estas informações podem ser de diferentes tipos e origens: banco de dados, programas, emails ou mesmo um site.

A empresa que disponibiliza este tipo de serviço, deve visar totalmente a questão da segurança de dados, tanto no armazenamento de informações, como na transmissão destas. Isto implica em manter um conjunto de requisitos básicos, desejáveis para garantir um alto nível de segurança para seus clientes.

9.5 – Requisitos básicos para hospedagem segura.

- **Pessoal técnico.** A empresa que oferece o serviço de hospedagem segura deve manter em seu quadro de funcionários profissionais especializados na área de atuação, com grande destaque para a área de segurança de dados, segurança de redes e sistemas operacionais.

- **Infra-estrutura de segurança.** Para oferecer um serviço de segurança satisfatório é necessário possuir uma infra-estrutura adequada e atualizada, dispondo das ferramentas estudadas nos capítulos 7 e 8.

- **Quantidade restrita de clientes.** A quantidade de clientes que a empresa de hospedagem pode ter deve ser proporcional à quantidade de funcionários que a empresa possui. Sobrecarregar os funcionários, atribuindo-lhes um número de clientes além do desejável, pode implicar em perda de confiabilidade no serviço prestado.

- **Dominar o processo**. A empresa de hospedagem não pode permitir que a administração da segurança dos dados fique a cargo do cliente. Se o cliente procura por um serviço de hospedagem segura, justamente por não possuir os mecanismos necessários à segurança, não é concebível que a administração das ferramentas de segurança fique sob o domínio deste.

9.6 – Casos práticos.

O serviço de hospedagem oferece recursos que muitas empresas tem dificuldade de implementar por conta própria, principalmente nos aspectos relacionados à segurança, seja esta física ou lógica.

Assim sendo, mesmo grandes empresas, que possuem recursos disponíveis para investimentos vultosos, têm optado pelo serviço de hospedagem. Entre estas empresas, pode-se citar os seguintes casos: Grupo Pão de Açúcar, Redecard, Xerox, etc.

Por outro lado, a solução de hosting também está aberta a empresas menores. Afinal, com preços que variam de R$ 12,90 a R$ 499,90 mensais é possível dispor de um ambiente de hospedagem segura [86], inclusive com suporte ao protocolo SSL.

Entre as empresas que oferecem o serviço de hospedagem e soluções para o comércio eletrônico, as opções também são heterogêneas, indo desde aquelas que trabalham basicamente com hospedagem, como a Meganick [86] e Optiglobe [87], até gigantes corporativas como a IBM [88].

CONCLUSÃO

Este capítulo procura relacionar os capítulos anteriores, demonstrando a linha de raciocínio que norteou esta pesquisa e conclui sobre a situação problema destacada na introdução e estudada ao longo dos capítulos.

Como foi demonstrado no primeiro capítulo, a Internet não surgiu de forma planejada. Tão pouco, o crescimento exponencial no número de usuários e a variedade de aplicações existentes, eram objetivados quando do seu surgimento.

Com uma origem militar, a Internet passou a ser utilizada em centros de pesquisas e universidades, chegando às empresas e a milhões de lares no mundo todo.

Este crescimento gigantesco, porém anárquico, da Internet, permite analisar vários aspectos resultantes, que não constavam nos objetivos iniciais dos idealizadores da Internet. Dentre estes aspectos, esta dissertação identificou e destacou dois aspectos distintos:

1 – O incremento do comércio eletrônico (capítulo 2) que possibilitou às empresas utilizarem a Internet como ponto de venda para seus produtos, servindo assim como um canal direto e de fácil acesso a milhões de usuários espalhados pelo mundo. Também de forma semelhante, as empresas podem utilizar a Internet para trocarem informações comerciais entre si e com seus parceiros comerciais.

2 – Outro aspecto, que pode-se adjetivar como negativo, é que a anarquia predominante na Internet, torna-a sujeita as ações de indivíduos mal-intencionados. Estas pessoas, genericamente denominadas hackers, (capítulo 3) se valem da facilidade de acesso da Internet e da fragilidade do protocolo de comunicação

utilizado, para implementar ações que comprometem o funcionamento dos sites das empresas e que podem ser danosas ao comércio eletrônico.

Portanto, para que o comércio eletrônico seja viável do ponto de vista da segurança, uma série de garantias deve existir. Elas foram abordadas de forma minuciosa no capítulo 4. Também foram abordados, no capítulo 5, os riscos e métodos de ataques que podem comprometer seriamente estas garantias e, por conseqüência, comprometer o comércio eletrônico

No capítulo 6 foram demonstrados os fundamentos de segurança para a transmissão segura de dados na Internet. Com base nestes fundamentos, foram analisados, no capítulo 7, as ferramentas que possibilitam a transmissão segura de dados.

Dentre estas ferramentas, foi destacada, no capítulo 8, o protocolo HTTPS, que é o principal método de implementação de transmissão segura de dados na Internet, sendo largamente utilizado por bancos e lojas virtuais.

No capítulo 9 foi demonstrado que todo o aparato necessário para o comércio eletrônico pode ser disponibilizado por empresas terceirizadas, denominadas IDC (Internet Data Center).

Estas empresas são prestadoras de serviços, especializadas em manter uma infra-estrutura voltada para a hospedagem de sites. Também pode fazer parte destes serviços a disponibilização dos conceitos de segurança estudados nesta dissertação.

Desta forma através do conceito de hospedagem segura, é possível disponibilizar as ferramentas de segurança para as empresas, que queiram implementar o comércio eletrônico.

A principal contribuição deste trabalho é mostrar que uma empresa que objetive implementar qualquer uma das formas de comércio eletrônico existentes pode, do ponto de vista da segurança, atingir este objetivo. Mesmo que a empresa não disponha de uma infra-estrutura adequada de informática, ela pode ter acesso a toda tecnologia disponível, através da contratação de empresas que oferecem hospedagem segura.

Outra contribuição deste trabalho é representada pela leitura básica sobre o assunto enfocado, uma vez que este não se prendeu apenas a analisar o problema, mas também a levantar o histórico e os fundamentos da Internet, bem como, a discutir e traçar perspectivas sobre o comércio eletrônico e os aspectos de segurança envolvidos.

Como sugestão de futura pesquisa, é deixada a questão da logística envolvida para a implementação do comércio eletrônico na modalidade B2C (negócio a cliente). Este trabalho analisou apenas os aspectos de segurança envolvidos no comércio eletrônico, porém, para o B2C, o comércio eletrônico não pode se limitar apenas à venda e ao recebimento do pagamento pelo produto vendido, mas também garantir a entrega do produto e o pós-venda.

BIBLIOGRAFIA

[1] KATAGIRI, Iao. Rand History´s: 50 years of service to the nation. *http://www.rand.org/history/.*

[2] BARAN, Paul. (1964) Introduction to distributed communications network. *http://www.rand.org/publications/RM/RM3420/*.

[3] LEINER, Barry M. (2000) All about the Internet: a brief history of the Internet. *http://www.isoc.org/internet/history/brief.shtml*.

[4] TANENBAUM, Andrew S. *Redes de computadores*, 4ª ed. Rio de Janeiro: Campus, 1997.

[5] INTERNET SOCIETY. (2000) *http://www.isoc.org/.*

[6] COMITÊ GESTOR DA INTERNET NO BRASIL. (2001) *http://www.cg.org.br/.*

[7] MANDEL, Arnaldo, SIMON, Imre, LYRA, Jorge, de. Informação: computação e comunicação. *Revista da USP*, São Paulo: Universidade de São Paulo, 1997.

[8] COMER, Douglas E. *The Internet book: Everything you need to know about computer networking and how de Internet works.* New Jersey: Prentice Hall, 1994.

[9] WALSH, Norman. (1998) A technical introduction to XML. *http://www.xml.com/pub/a/98/10/guide0.html.*

[10] KROL, Ed. *The whole Internet*, 2ª ed. Califórnia: O´Reilly & Associates, 1994.

[11] CERN EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH. (1998) The World Wide Web*. http://public.web.cern.ch/Public/ACHIEVEMENTS/web.html.*

[12] MESQUITA, Renata. (2001) Já somos 11,9 milhões de internautas. *Info Exame*, 2001. *http://www2.uol.com.br/info/aberto/infonews/082001/10082001-16.shl.*

[13] COMITÊ GESTOR DA INTERNET NO BRASIL. (2002) Indicadores. *http://www.cg.org.br/indicadores/index.htm/.*

[14] ZWASS, Vladimir. *Foundations of information system.* UK: IE-Mcgraw-Hill, 1998.

[15] CLARKE, Roger. (1999) Eletronic commerce definitions. *http://www.anu.edu.au/people/Roger.Clarke/EC/ECDefns.html.*

[16] KALAKOTA, Ravi, WHISTON Andrew B. *Eletronic commerce: a manager's guide.* Addison Wesley, 1997.

[17] GOVERNO ELETRÔNICO. (2002) Histórico. *http://www.governoeletronico.gov.br/index.*

[18] SUBRAMANIAN, Srividhya. *Design and verificarion of secure e-commerce.* Ohio: The Ohio State University, 1999.

[19] KATERATTANAKUL, Pairin. *Development of an instrument for assessing quality of the web site for Internet Business: A structural modeling approach*. University of Nebraska, 2000.

[20] KOTLER, Philip. *Administração de marketing,* 5ª ed. São Paulo: Atlas, 1992.

[21] SANTOS, Rubens C. *Comércio eletrônico: Uma oportunidade para estreitar o relacionamento entre consumidores e empresas?* São Paulo: Fundação Getúlio Vargas, 1999.

[22] COLE Patrick E. e outros. Internet: o comércio eletrônico. *Folha de São Paulo*, São Paulo, 16.6.1998. Suplemento Time, Vol.1 Nº 16.

[23] INTERSIX TECHNOLOGIES.(2000) Analisando o momento atual. *http://www.intersix.com.br/portugues/seguranca/analisando.htm.*

[24] IDG NOW!. (2002) E-commerce no Brasil está crescendo, diz USP. *http://idgnow.terra.com.br/idgnow/ecommerce/2002/09/0005.*

[25] IDG NOW!. (2002) Brasil lidra e-business na América Latina. *http://idgnow.terra.com.br/idgnow/ecommerce/2002/09/0003.*

[26] BRUNER, Rick E. *Net results, o marketing eficaz na web*. São Paulo: Quark do Brasil, 1998.

[27] ASSOCIAÇÃO NACIONAL DOS PERITOS CRIMINAIS FEDERAIS. (2001) A nova face do crime. *http://www.apcf.org.br/especial.htm.*

[28] GREGO, Maurício. O submundo dos hackers. *Info Exame*, São Paulo, ano 15 nº 173: 46-58, ago.2000.

[29] OUSADIA marca a ação dos crackers e hackers. *Diário Popular*, São Paulo, 17.07.2001. Caderno de Informática, p. 4.

[30] VIEIRA, Eduardo. Os donos do e-commerce. *Info Exame*, São Paulo, ano 17 nº 194: 64-77, mai.2002.

[31] ZANINOTTI, Thiago. (2000) Síndrome de impunidade persiste. *http://www.securenet.com.br/artigo.php?artigo=76.*

[32] SILVA, Alessandro. Aumento de furtos on-line mobiliza polícia. Folha de São Paulo, São Paulo, 9.9.1999. Caderno São Paulo, p. 8.

[33] PIMENTA, Angela. Os hackers não são engenhosos. *Veja*, São Paulo, ano 33 nº 16. Suplemento Veja Digital, p. 71.

[34] CERTISIGN. (1999) Securing your web site for business. *https://www.certisign.com.br/respostas/1/guia.zip.*

[35] GUIZZO, Érico. (2001) Negócios Exame. *http://www.uol.com.br/negociosexame/revista/revista0009_16.html.*

[36] MÓDULO SECURITY SOLUTIONS S.A. *Sétima pesquisa nacional sobre segurança da informação*, jul.2001.

[37] BASTOS, ALBERTO. *Os novos rumos da gestão de segurança com as normas ISO 17799 e BS 7799.* Módulo security magazine, Ago.2002.

[38] CLARKE, Roger. (1999) Introduction to dataveillance and information privacy, and definitions of terms. *http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.*

[39] CLARKE, Roger. (1998) Message transmission security: or 'cryptography in plain text'*. http://www.anu.edu.au/people/Roger.Clarke/II/CryptoSecy.html.*

[40] CLARKE, Roger. (1998) Message transmission security risks*. http://www.anu.edu.au/people/Roger.Clarke/II/CryptoSecyRisks.html*

[41] REZENDE, Pedro Antonio Dourado de. *Redes abertas e fechadas, riscos com as tecnologias atuais*. In: Simpósio E-Dia, Colégio Notarial do Brasil, ANOREG e Ordem dos Advogados do Brasil. São Paulo, 19.09.2000.

[42] NETSEC, Internet Security. (2000) Engenharia social. *http://www.netsec.com.br/tecnologia/engenharia_social.htm.*

[43] FIGUEIREDO, Antonio. (2000) Administração de sistemas e segurança: sniffers. *http://www.revista.unicamp.br/infotec/admsis/admsis8-1.html.*

[44] REDE NACIONAL DE PESQUISA. (2000) Tudo que você precisa saber sobre os ataques DdoS. *http://www.rnp.br/newsgen/0003/ddos.shtml.*

[45] ANONYMOUS*. Maximum security: A hacker´s guide to protecting your internet site and network*. Indiana: Sams,1998.

[46] KEYBOARD MASTERS TEAM.(2002). Spoofing do IP. *http://www.km-team.com/papers/ip.htm*

[47] SHIREY, R. (2000) Internet security glossary RFC 2828. *http://ietfreport.isoc.org/rfc/rfc2828.txt.*

[48] DAVIES, D. W, PRICE, W.L., *Security for computer networks*. Chicester: John Wiley & Sons, 1984.

[49] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (1980) DES: modes of operation. *http://www.itl.nist.gov/fipspubs/fip81.htm.*

[50] MEDIACRYPT.(2001) IDEA Algorithm. *http://www.mediacrypt.com/engl/Content/ideaTM_algorithm.htm.*

[51] VERISIGN. (2000) Understanding public key infrastructure: PKI. *htttp://verisign.netscape.com/security/pki/understanding.html.*

[52] RSA Security Inc. (2001) *http://www.rsasecurity.com/.*

[53] LUCCHESI, Claudio L. *Introdução à criptografia*. Universidade estadual de Campinas, 1984.

[54] RIVEST, R. (1992) The MD5 Message-Digest algorithm RFC 1321. *http://ietfreport.isoc.org/rfc/rfc1321.txt.*

[55] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (1995) Secure hash standard. *http://www.itl.nist.gov/fipspubs/fip180-1.htm*.

[56] COMPUTER EMERGENCY RESPONSE TEAM - RS. (2000) Assinaturas digitais: funções de hash. *http://www.cert-rs.tche.br/docs_html/autentic.html.*

[57] IDG NOW!. (2001) Senado brasileiro aprova lei de assinatura digital. *http://idgnow.terra.com.br/idgnow/internet/2001/05/0087.*

[58] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2002) The Keyed-Hash message authentication code (HMAC). *http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf.*

[59] INTERSIX TECHNOLOGIES. (2000) Certificados e assinaturas digitais. *http://www.intersix.com.br/portugues/seguranca/controleacesso.htm.*

[60] SILVA, Fernando J. A. A auditoria de informática face ao comércio eletrônico através da Internet: Um estudo no setor financeiro. São Paulo: Universidade de São Paulo, 2000.

[61] REDE NACIONAL DE PESQUISA. (1999) Política de segurança. *http://www.rnp.br/newsgen/9909/politica.shtml.*

[62] FRASER, B. (1997) Site Security Handbook RFC 2196. *http://ietfreport.isoc.org/rfc/rfc2196.txt.*

[63] CHESWICK, William, R., BELLOVIN, Steven M. *Firewalls and Internet security.* Massachusetts: Addison Wesley, 1994.

[64] ZWICKY, Elizabeth D., COOPER, Simon. *Building Internet firewalls.* Massachusetts: O'Reilly, 2000.

[65] NIC BR SECURITY OFFICE. (2002) Práticas de segurança para administradores de redes Internet. *http://www.nbso.nic.br/docs/seg-adm-redes.pdf.*

[66] KENT, S. (1998) Security architecture for the Internet protocol RFC 2401. *http://ietfreport.isoc.org/rfc/rfc2401.txt.*

[67] REDE NACIONAL DE PESQUISA. (1998) Rede privada virtual - VPN. *http://www.rnp.br/newsgen/9811/vpn.shtml.*

[68] VISA, MASTERCARD*. SET Secure electronic transaction specification, Book 1: business description*, 1997.

[69] VERISIGN. (2002) CyberCash cashregister support documentation. *http://www.verisign.com/support/cyberCash/supportDocs.html.*

[70] EASTLAKE, D. e outros. (1996*) CyberCash credit card protocol version 0.8. RFC1898. http://ietfreport.isoc.org/rfc/rfc1898.txt.*

[71] HUFF, Sid, WADE, Michael. (1999) First Virtual Holdings Incorporated. *http://www.uncc.edu/icis99/program/TC9903.PDF.*

[72] NETCHEQUE. (2002) *The NetCheque network payment system*. *http://www.netcheque.org/.*

[73] NEUMAN, B., Cliford, MEDVINSKY, Gennady. *Requirements for network payment: the NetCheque perspective*, Information Sciences Institute University of Southern California, 1995.

[74] ECHECK. (2002) Echeck overview. *http://echeck.commerce.net/overview/index.html*

[75] STALLINGS, WILLIAN. *Mecklermedia´s official Internet world*. California: IDG Books, 1995.

[76] GHOSH, Anup K. E-Commerce security. New York: John Wiley & Sons, 1998.

[77] MONDEX. (1996) All about Mondex. *http://www.mondex.com/*

[78] INTERNET ASSIGNED NUMBERS AUTHORITY (2001). Port numbers. *http://www.iana.org/assignments/port-numbers*

[79] THOMAS, Stephen*. SSL and TLS essentials: Secure the web.* New York: John Wiley & Sons, 2000.

[80] FREIER, Alan, KARLTON, Philip, KOCHER, Paul. (1996) The SSL protocol version 3.0. *http://wp.netscape.com/eng/ssl3/draft302.txt.*

[81] DIERKS, T., ALLEN, C. (1999) The TLS protocol version 1.0. *http://ietfreport.isoc.org/rfc/rfc2246.txt*

[82] NETSCAPE COMMUNICATIONS CORPORATION. (1997) Chapter 14 Understanding encryption and SSL.
http://developer.netscape.com/docs/manuals/proxy/adminux/encrypt.htm

[83] FORESTI, Nivaldo. (2001) Data Centers: na mira do e-business.
http://www.itweb.com.br/shared/print_story.asp?id=10357.

[84] LUNE NETWORKS. (2002) Hosting seguro.
http://www.lunenetworks.com.br/frames.html?target=servicos.html.

[85] DIGISENSOR SISTEMAS DE SEGURANÇA. (2002) Combate a incêndios por gás FM-200. *http://www.digisensor.com.br/digisensor3a2.html.*

[86] MEGANICK PRESENCE PROVIDER. (2002) Hospedagem de web sites.
http://www.meganick.com.br/.

[87] OPTIGLOBE TELECOMUNICAÇÕES S/A. (2002) Optiglobe Communications.
http://www.optiglobe.com.br/.

[88] IBM BRASIL. (2002) IBM e-business home page.
http://www-3.ibm.com/e-business/br/index.shtml

BIBLIOGRAFIA COMPLEMENTAR

ALBERTIN, Luiz A. Comércio eletrônico: modelo, aspectos e contribuições de sua aplicação. São Paulo: Atlas, 2000.

BOTTONI, Fernanda. (2001) 59% das empresas já estão online. *Info Exame*, 2001. *http://www2.uol.com.br/info/aberto/infonews/082001/09082001-19.shl.*

CAILLIAU, Robert. (1995) A little history of the World Wide Web. *http://www.w3.org/History.html.*

CENTRO BRASILEIRO DE ESTUDOS JURÍDICOS DA INTERNET. (2001) A assinatura digital é assinatura formal. *http://www.cbeji.com.br/artigos/artcartorio_assformal.htm*

CENTRO BRASILEIRO DE ESTUDOS JURÍDICOS DA INTERNET. (2001) Regulamentação da certificação eletrônica. *http://www.cbeji.com.br/artigos/artdouglas21082001.htm.*

CHOR, Ben-Zior. *Two issues in public-key cryptography*. Massachusetts: The Mit Press, 1985.

CLARKE, Roger. (2001) Can digital signatures and public key infrastructure be of any use in the health care sector ? *http://www.anu.edu.au/people/Roger.Clarke/EC/PKIHlth01.html*

CLARKE, Roger. (1996) Privacy issues in smart card applications in the retail financial sector. *http://www.anu.edu.au/people/Roger.Clarke/EC/PKIHlth01.html.*

COMPUTER EMERGENCY RESPONSE TEAM. (1995) IP Spoofing attacks and hijacked terminal connections. Advisory CA-1995-01. *http://www.cert.org/advisories/CA-1995-01.html.*

CORRÊA JUNIOR, Isvi. *Uma implementação do protocolo TLS com um algoritmo de criptografia forte*. Universidade de São Paulo, 2002.

DENNING, Dorothy E. R. *Cryptography and data security.* Massachusetts: Addison-Wesley, 1982.

GARFINKEL, Simson, SPAFFORD, Gene. Web Security & Commerce. California: O´Reilly & Associates, 1997.

HOULE, Kevin J., WEAVER, George M. (2001)Trends in denial of service attack technology. CERT Coordination Center. *http://www.cert.org/archive/pdf/DoS_trends.pdf.*

KROL, Ed, HOFFMAN Ellen. (1993) What is the Internet? RFC1462.
http://ietfreport.isoc.org/rfc/rfc1462.txt.

LAKATOS, Eva M., MARCONI, Marina A. *Metodologia do trabalho científico*, 5ª ed. São Paulo: Atlas,2001.

MEADOWS, Catherine.(2001) A framework for Denial of Service analysis. Naval Research Laboratory. http://www.cert.org/research/isw/isw2000/papers/37.pdf.

NETSEC, Internet Security. (2000) Ip Spoofing.
http://www.netsec.com.br/tecnologia/IP_spoofing.htm.

REDE NACIONAL DE PESQUISA. (1998) A nova geração de protocolos IP.
http://www.rnp.br/newsgen/9811/intr-ipv6.shtml

SAVARD, John J. G. (1999) Improving Substitution.
http://home.ecn.ab.ca/~jsavard/crypto/pp0103.htm.

SAVARD, John J. G. (1999) Methods of transposition.
http://home.ecn.ab.ca/~jsavard/crypto/pp0102.htm.

SEVERINO, Antonio J. *Metodologia do trabalho científico*. São Paulo: Cortez, 2001.

SILBERSCHATZ, Abraham, GALVIN, Peter B. *Sistemas operacionais conceitos*. São Paulo: Prentice Hall, 2000.

SOUSA JR., Rafael de, PUTTINI, Ricardo. (2001) RSA - Rivest, Shamir and Adleman algorithm. *UnB - Departamento de Engenharia Elétrica.*
http://www.redes.unb.br/security/criptografia/rsa/rsa.html.