Ensaios e Ciência: Ciências Biológicas, Agrárias e da Saúde
ISSN: 1415-6938
editora@uniderp.br
Universidade Anhanguera
Brasil

Silva, Francisco José; Almeida Leitum de, Waldeci
SEGURANÇA NA WEB
Ensaios e Ciência: Ciências Biológicas, Agrárias e da Saúde, vol. 4, núm. 1, abril, 2000, pp. 115-136
Universidade Anhanguera
Campo Grande, Brasil

Segurança Na *Web*

Francisco José Silva
Waldeci Leitun de Almeida

e-mail: franciscojosilva@aol.com
e-mail: waldeci@trt24.gov.br
UNIDERP – Universidade para o Desenvolvimento do Estado e da Região do Pantanal
Coordenadoria de Ciência da Computação, Processamento de Dados
e Engenharia da Computação

RESUMO

Este texto abordará os fundamentos da segurança na *Web*. Tal segurança é usada para proteger os servidores, usuários e suas empresas contra o comportamento inesperado, através de técnicas de identificação digital, utilização de *firewalls*, chaves públicas e privadas, criptografia, utilização de protocolos para ambientes de correio e comércio eletrônico. São descritas as principais características dos protocolos PGP, SSL e SET e suas utilizações.

Palavras-chave:

Internet, segurança das informações, identificação digital, criptografia.

ABSTRACT

This text describes the principles of Web security. This security is used to protect the servers, the users and their companies against the unexpected behavior, through digital identification techniques, the use of firewalls, private and public keys, cryptography, the use of protocols for e-mail and electronic commerce environments. The main characteristics of PGP, SET and SSL protocols and their applications are described on this paper.

Key-words:

Internet, information security, digital identification, cryptography.

1 INTRODUÇÃO

A Internet tem despontado como o grande veículo dos tempos modernos. Os números da rede impressionam: há cerca de 320 milhões de usuários no mundo e 4,9 milhões no Brasil. A projeção é de que haja 720 milhões de usuários Internet no mundo em 2003. Os negócios estão se modernizando, a tecnologia está assumindo o status merecido e a *Web* já faz parte do cotidiano corporativo (Sêmola, 1999).

Dentro da evolução natural das empresas, o *e-security* representa o próximo passo. É a gestão corporativa da segurança. A gestão inteligente das informações, pessoas, processos, infra-estrutura, aplicações e tecnologia garantindo a segurança dos dados estratégicos e viabilizando o sucesso na integração entre tecnologia e negócio.

O termo *e-business* surgiu a partir da utilização de computadores na interligação de empresas, estabelecendo a comunicação *business-to-business* e integrando a cadeia de valor.

A troca de informações por meio eletrônico entre o computador do vendedor e o micro do consumidor recebe o nome de *e-commerce*. Em princípio, qualquer meio de comunicação é válido para implementar estas práticas: redes privadas ou públicas, com qualquer característica física ou lógica. Contudo, a Internet tem despontado como o grande veículo dos tempos modernos, graças a sua abrangência global, tecnologia difundida e documentada, além do custo reduzido.

Durante o 2º Congresso Nacional sobre Segurança e Auditoria da Informação ocorrido em São Paulo, nos dias 10 e 11 de setembro de 1999, foi realizada a 4ª pesquisa nacional sobre segurança da informação, que envolveu 176 empresas de várias localidades do país e diversas áreas de atuação como instituições financeiras, empresas de serviços e telecomunicações, universidades e entidades do governo.

Das empresas ouvidas, 87% consideram que a segurança das informações é estratégica. Entretanto, apenas 67% delas possuem uma

política de segurança formalizada, sendo que, desse total, 69% seguem regras desatualizadas, que não contemplam todos os ambientes ou não são conhecidas pelos usuários. Os tópicos mais abordados por tais políticas dizem respeito ao uso de software, vírus de computador e uso de senhas, que reúnem 70% do interesse.

O número de empresas que usa *firewall* também aumentou consideravelmente em relação ao ano anterior. De 18% em 97 para 45%, 1999. A preocupação maior está relacionada ao vazamento de informações sigilosas e fraudes em mensagens utilizadas para operações e transações de negócios. Os resultados da pesquisa estão demonstrados na figura 1.

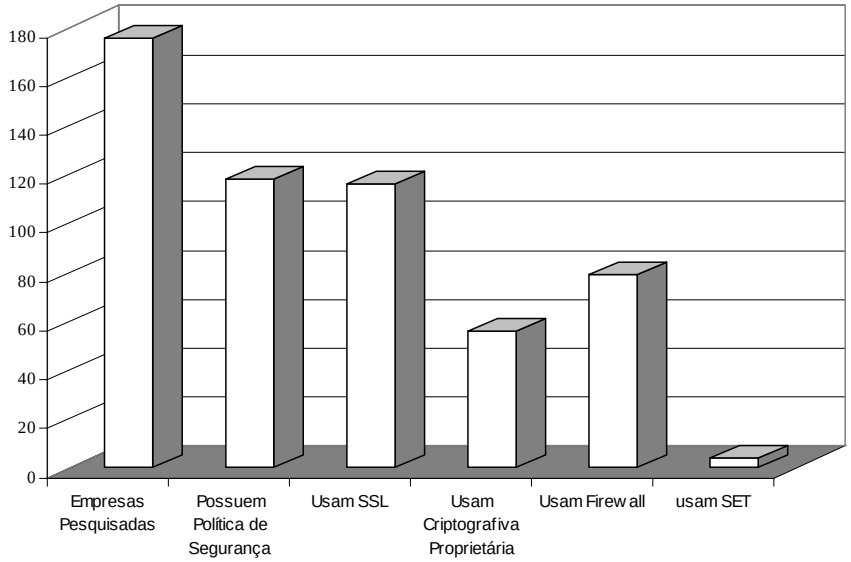

Figura 1 - 4ª Pesquisa Nacional sobre Segurança da Informação

Fonte: Corrêa, 1999

2 SEGURANÇA DAS INFORMAÇÕES NAS EMPRESAS

As principais vulnerabilidades encontradas costumam ser relativas a erros, acidentes ou desconhecimento dos usuários que, inadvertidamente, alteram configurações de equipamentos, divulgam contas e senhas de acesso, deixam sessões abertas na sua ausência, utilizam senhas frágeis facilmente descobertas (como o próprio nome ou palavras comuns) ou mesmo contaminam seus arquivos e programas com vírus de computadores. (Garfinkel & Spafford, 1998).

Os criminosos estão se aperfeiçoando com técnicas e ferramentas para violar os sistemas das empresas, praticar vandalismo, cometer fraudes, extorsões e roubo de informações. Os princípios básicos da segurança são a confidencialidade, integridade e disponibilidade das informações.

2.1 AMEAÇAS E VULNERABILIDADES

O uso de Internet nas empresas trouxe novas vulnerabilidades na rede interna. Se não bastassem as preocupações existentes com espionagem industrial, fraudes, erros e acidentes, as empresas precisam se preocupar agora com os *hackers*, invasões, vírus, cavalos de tróia e outras ameaças que penetram através desta nova porta de acesso. Para obter segurança em uma aplicação para Internet ou Intranet, é preciso cuidar de quatro elementos básicos: segurança na estação (cliente), segurança no meio de transporte, segurança no servidor, segurança na Rede Interna (Azevedo, 1999).

2.1.1 Segurança na Estação

No uso de Internet e Intranet, um dos elementos mais vulneráveis sem dúvida é a estação, onde normalmente é executado um *browser* ou uma aplicação dedicada por onde o usuário tem acesso aos recursos e serviços da rede (Corrêa, 1999).

As estações dos usuários podem armazenar chaves privadas e

informações pessoais na maioria das vezes sem proteção ou controle de acesso.

Estações de trabalho estão ainda sujeitas a execução de programas desconhecidos (como *Applets Java*, *ActiveX* e *Javascripts*) sendo expostas a grampos de teclado e outras armadilhas de ganho de acesso.

Existem ainda diversos usuários que fazem uso de modems para conexão com a Internet, muitas vezes contornando os controles e proteções da rede ou de um *firewall* corporativo.

2.1.2 Segurança no Meio de Transporte

Para garantir a privacidade e integridade das informações enviadas pela Internet / Intranet, é necessário implementar a segurança no meio de transporte. A criptografia é fundamental para este fim, sendo que os principais produtos que possuem criptografia "embutida" sofrem limitações por causa das restrições de exportação dos EUA.

2.1.3 Segurança nos Servidores

O uso de Internet / Intranet exige ainda segurança nos servidores.

As empresas têm conectado sua rede interna à Internet mas não gostariam de conectar a Internet à rede interna. Para isto, torna-se necessário o uso de *firewalls* que protegem o acesso através de um servidor de controle no ponto único de entrada/saída dos dados.

2.1.4 Segurança na Rede Interna

Finalmente, a segurança deve prever a proteção e controle da Rede Interna. O modelo atual para segurança das redes tem assumido que o "inimigo" está do lado de fora da empresa, enquanto dentro, todos são confiáveis. Esta idéia tem feito que os desenvolvedores de sistemas e administradores de rede utilizem uma estratégia simplista na Internet evitando qualquer acesso externo e, por outro lado, liberando o acesso irrestrito aos servidores para usuários internos. (Garfinkel & Spafford, 1999).

A solução completa abrange: Política de Segurança Corporativa com

definição clara das diretrizes, normas, padrões e procedimentos que devem ser seguidos por todos os usuários; Programa de treinamento e capacitação dos técnicos e usuários; Recursos e ferramentas específicas para a segurança.

3 FIREWALLS

Um *firewall* é um dispositivo (geralmente um computador que executa um sistema operacional modificado ou especialmente escrito) que isola uma rede interna de empresas conectadas à Internet, permitindo que conexões específicas liberem e bloqueiem outras redes. Teoricamente, os *firewalls* são configurados para que todas as conexões externas a uma rede interna passem por poucos locais relativamente bem monitorados. O conceito de *Firewall* é de um filtro de pacotes, permitindo estabelecer regras para a entrada e saída de pacotes de uma rede. Geralmente é implementado em um roteador, ou em computador que está exercendo o papel filtro para o roteador. Os *firewalls* de *gateway* tradicionais foram desenvolvidos especificamente para proteger as redes de invasões externas, provenientes da Internet pública. O principal objetivo de tais produtos é controlar o acesso de fontes externas à sua rede privada. Deste modo, os *firewalls* fazem parte de uma estratégia de segurança geral de uma empresa. (Garfinkel, 1999).

Um *firewall* deve ser usado somente para oferecer uma segurança adicional que funcione em conjunto com controles internos - e nunca como um substituto para eles.

4 TÉCNICAS DE IDENTIFICAÇÃO DIGITAL

Uma maneira para se comprovar a identidade no mundo físico é carregar credenciais de um órgão confiável. Elas também devem ser à prova de falsificação para evitar que alguém que não seja o governo ou organização confiável as emitam. Da mesma forma, em sistemas computacionais existem diversas técnicas de identificação digital baseadas em senhas, tokens físicos

(cartões de acesso), medidas biométricas ou localização. (Garfinkel, 1999).

Muitos dos sistemas de identificação citados podem ser melhorados por meio da utilização de assinaturas digitais. Resumidamente, cada usuário de um sistema de assinatura digital cria um par de chaves:

· Uma chave particular: usada para representar uma assinatura digital em um bloco de dados, como um documento HTML, uma mensagem eletrônica ou uma fotografia.

· Uma chave pública: usada para verificar uma assinatura depois que ela foi feita.

A técnica do par de chaves é mostrada na figura 2, comunicação entre dois usuários.

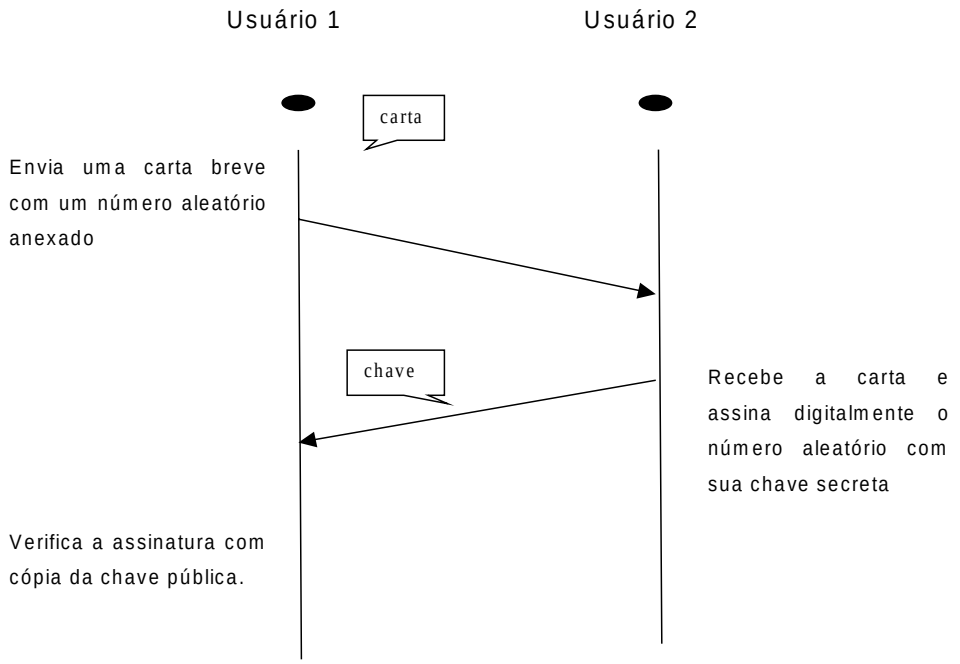

Figura 2 - Usando uma assinatura digital para provar quem você é.

4.1 CHAVES PARTICULAR E PÚBLICA

Apesar de ser possível, na teoria, memorizar sua chave particular, na maioria dos casos estas são armazenadas em computador, pois, para serem seguras, são muito grandes e portanto difíceis de memorizar.

Elas podem ser armazenadas:

a) criptografadamente no disco rígido: a desvantagem é que se alguém consegue acesso ao seu computador e sabe sua expressão de senha, esta pessoa pode acessar sua chave particular;

b) criptografadamente em meio removível: em razão de a chave ser colocada na memória do computador para criptografia, tanto neste modo, como no anterior, as chaves são vulneráveis a ataques por vírus de computador, cavalo de tróia ou outro programa mal-intencionado;

c) em um *smart card* ou em outro dispositivo inteligente: esta é uma das maneiras mais seguras de proteger a sua chave particular. O cartão inteligente tem um pequeno microprocessador e é capaz de criar um par de chaves particular/pública. O cartão inteligente pode transmitir a chave pública para o computador *host* e tem uma quantidade limitada de espaço de armazenamento para conter 10 ou 20 certificados de chave pública. Teoricamente, a chave particular nunca sai do cartão. Em vez disto, se você deseja assinar ou decodificar um trecho de informação, o mesmo deve ser transmitido para dentro do cartão, e a resposta assinada ou decodificada deve ser transmitida para fora do cartão. Assim, os *crackers* não podem usar sua chave particular, a menos que eles se apossem do seu cartão inteligente, pois a própria chave nunca é colocada na memória do computador.

5 CRIPTOGRAFIA

Criptografia representa um conjunto de técnicas que são usadas para manter a informação segura. Usando a criptografia, é possível transformar palavras escritas ou outros tipos de mensagens, de forma a ficarem ininteligíveis para receptores não autorizados. Um receptor autorizado pode transformar as palavras ou a mensagem em uma mensagem perfeitamente compreensível (decifragem).

Há dois tipos básicos de algoritmos de criptografia em uso atualmente:

a) Algoritmos de chave simétrica: onde a mesma chave é utilizada para criptografar e decifrar a mensagem. Eles são chamados às vezes de algoritmos de chave secreta ou de chave privada.

b) Algoritmos de chave pública: esses algoritmos usam uma chave para criptografar a mensagem e outra para decifrá-la. A chave de criptografia é chamada de chave pública, pois pode ficar disponível sem comprometer o segredo da mensagem, nem a chave de decifragem. A chave de decifragem é chamada de chave secreta ou privada. Sistemas de chave pública são chamados, às vezes, de algoritmos de chave assimétrica.

5.1 ALGORITMOS DE CHAVE SIMÉTRICA

Os algoritmos de chave simétrica podem ser divididos em duas categorias: de bloco e de fluxo. Algoritmos de bloco criptografam os dados um bloco de cada vez, enquanto os algoritmos de fluxo criptografam *byte* por *byte*.

Alguns dos algoritmos mais comuns no campo da segurança na *Web* são resumidos na lista a seguir: (Garfinkel, 1999)

a) DES (*Data Encryption Standard*): Foi adotado como padrão pelo governo dos EUA em 1977, e como padrão ANSI em 1981. O DES é um algoritmo de bloco que usa uma chave de 56 bits e tem diferentes modo de operação, dependendo da finalidade com que é usado.

b) DESX: É uma simples modificação do algoritmo DES, construída em duas etapas. Estas etapas visam melhorar a segurança do algoritmo,

tornando a busca da chave praticamente impossível.

c) Triple-DES: O *Triple*-DES é uma maneira de tornar o DES pelo menos duas vezes mais seguro, usando o algoritmo de criptografia três vezes, com três chaves diferentes. Usar o DES duas vezes com duas chaves diferentes não aumenta a segurança tanto quanto poder-se-ia pensar, por causa de um tipo teórico de ataque conhecido como "*meet-in-the-middle*", com o qual o atacante tenta criptografar o texto limpo simultaneamente com uma operação do DES e decifrar o texto com outra operação. Atualmente, o *Triple*-DES está sendo usado por instituições financeiras como uma alternativa para o DES.

d) *Blowfish*: É um algoritmo de criptografia em bloco, rápido, compacto e simples, inventado por Bruce Schneier. O algoritmo permite a utilização de uma chave de tamanho variável, até 448 bits, e é otimizado para executar em processadores de 32 ou 64 bits. Não é patenteado e foi colocado em domínio público.

e) RC2: O RC2 é fornecido com uma implementação que permite a utilização de chaves de 1 a 2048 bits. Muitas vezes o tamanho da chave é limitado a 40 bits no *software* vendido para exportação.

f) RC4: O RC 4 é vendido com uma implementação que permite a utilização de 1 a 2048 bits. O tamanho da chave é limitado a 40 bits no *software* vendido para exportação.

g) RC5: O RC5 permite que o tamanho da chave, o tamanho dos blocos de dados e o número de vezes que a criptografia será realizada sejam definidas pelo usuário (Garfinkel & Spafford, 1999).

5.2 ALGORITMOS DE CHAVE PÚBLICA

Os algoritmos de chave pública são baseados na teoria dos números.

O desenvolvimento de novos algoritmos de chave pública requer a identificação de novos problemas matemáticos com propriedades particulares. A lista a seguir apresenta os sistemas de chave pública atualmente em uso:

a) Troca de chaves de Diffie-Hellman: É um sistema para troca de chaves criptográficas entre partes. Na verdade, não é um método de criptografia ou decifragem, é um método para troca de chave privada compartilhada por meio de um canal de comunicação público. Com efeito, as duas partes estabelecem certos valores numéricos comuns, e cada uma delas cria uma chave. As transformações matemáticas das chaves são intercambiadas. Cada parte calcula então uma chave de sessão, que não pode ser descoberta facilmente por um atacante que conheça os valores intercambiados.

b) RSA: É um sistema de chave pública que pode tanto ser usado para criptografar informações, como para servir de base para um sistema de assinatura digital. A chave pode ter qualquer tamanho, dependendo da implementação usada.

c) ElGamal: É baseado no protocolo de troca de chaves Diffie-Hellman. Pode ser usado para criptografia e assinatura digital.

d) DDS (*Digital Signature Standard*): O Padrão de Assinatura Digital foi desenvolvido pela Agência Nacional de Segurança (NSA), e adotado como Padrão Federal de Processamento de Informação (FIPS) pela Instituto Nacional de Padrões e Tecnologia (NIST). O DDS é baseado no Algoritmo de Assinatura Digital - DSA - que permite a utilização de qualquer tamanho de chave, embora, na DSS FIPS só sejam permitidas entre 512 e 1024 bits. O DDS só pode ser usado para a realização de assinaturas digitais, embora haja implementações do DSA para criptografia.

5.3 FUNÇÕES DE CODIFICAÇÃO DE MENSAGEM

As funções de codificação de mensagem destilam a informação contida em um arquivo (grande ou pequeno) em um único número grande, geralmente entre 128 e 256 bits. Diversas funções de codificação de mensagem foram propostas e encontram-se em uso, sendo algumas delas:

a) HMAC (*Hashed Message Authentication Mode*): O Código de Autenticação de Mensagem Confusa é uma técnica que usa uma chave

secreta e uma função de codificação para criar um código secreto de autenticação de mensagem.

b) MD2 (*Message Digest* #2): Produz uma codificação de 128 bits.

c) MD4 (*Message Digest* #4): Foi desenvolvido como uma alternativa rápida ao MD2. É possível encontrar dois arquivos que produzem o mesmo código MD4 sem uma pesquisa de força bruta, sendo portanto pouco seguro. Produz uma codificação de 128 bits.

d) MD5 (*Message Digest* #5): É uma modificação do MD4 que inclui técnicas para torná-lo mais seguro. Embora largamente usado, foram descobertas algumas falhas que permitiam calcular alguns tipos de colisão. Como resultado sua popularidade vem caindo. O MD 5 produz uma codificação de 128 bits.

6 SISTEMAS CRIPTOGRÁFICOS ATUALMENTE EM USO

Os sistemas criptográficos em uso podem ser divididos em duas categorias. O primeiro grupo é o de programas e protocolos usados para criptografia de mensagens de correio eletrônico, tais como, o PGP. A segunda categoria de sistemas criptográficos é a de protocolos de rede usados para oferecer confidencialidade, autenticação, integridade e não-repúdio em ambientes de rede, tais como o SSL e o SET (Corrêa, 1999).

7 PGP

Um dos primeiros programas criptográficos de chave pública a se disseminar foi *Pretty Good Privacy*. O PGP oferece uma série de padrões que descrevem o formato das mensagens criptografadas, chaves e assinaturas digitais. (Holschuh, 1997).

É um sistema criptográfico híbrido que usa criptografia de chave pública RSA para gerenciamento de chave e criptografia simétrica IDEA para a cifragem dos dados brutos. O PGP oferece confidencialidade, por meio do algoritmo criptográfico IDEA; integridade, por meio da função MD5;

autenticação, pelos certificados de chave pública; e não-repúdio, por meio do uso de mensagens criptograficamente.

Um problema do PGP é o gerenciamento e a certificação de chaves públicas. As chaves do PGP nunca perdem a validade. Quando ficam comprometidas, cabe ao portador distribuir uma anulação especial da chave para todos com quem se comunica. Se for criada uma chave pública com o PGP e distribuí-la, deve-se resguardá-la sempre, porque ela nunca expira.

8 SSL

A SSL (*Security Socket Layer* – Camada de *Socket* de Segurança) é um protocolo criptográfico de uso geral para garantir a segurança em canais de comunicação bidirecionais. Geralmente é usado com o protocolo TCP/IP da Internet. A SSL é o sistema criptográfico usado por navegadores com o Netscape *Navigator* e o Internet *Explorer*, mas pode ser usado com qualquer serviço TCP/IP (Holschuh, 1997).

Enquanto o protocolo TCP/IP padrão tem apenas a função de enviar um fluxo de informações anônimo entre dois computadores (ou entre dois processos no mesmo computador), a SSL, sendo uma camada que existe entre o protocolo TCP/IP e o aplicativo, adiciona numerosos recursos a esse fluxo. Entre eles estão:

a) autenticação e não repúdio do servidor, usando assinaturas digitais;

b) autenticação e não repúdio do cliente, usando assinaturas digitais;

c) confidencialidade dos dados, por meio do uso de criptografia;

d) integridade dos dados, por meio de códigos de autenticação de mensagens.

A criptografia é um campo em constante mudança, e os protocolos criptográficos não funcionam, a não ser que ambas as partes usem os mesmos algoritmos. Por isso, a SSL é um protocolo que pode ser adaptado. Quando um programa SSL entra em contato com outro, os dois comparam

notas e determinam qual o protocolo mais poderoso que têm em comum. A troca é chamada de SSL *Hello*.

A SSL foi criada para ser usada no mundo todo, mas foi desenvolvida nos Estados Unidos e faz parte de programas vendidos por empresas norte-americanas para outros países. Por essa razão, muitos recursos foram criados em conformidade com a política restritiva do governo americano em relação à exportação de sistemas criptográficos. A SSL oferece muitos recursos, de interesse prático e teórico:

a) Separação de tarefas: A SSL usa algoritmos diferentes para criptografia, autenticação e integridade de dados, com chaves diferentes (chamadas segredos) para cada função. A vantagem principal dessa separação é que se podem usar chaves maiores para autenticação e integridade do que para privacidade. Isto é útil para produtos com destino à exportação, pois os regulamentos norte-americanos limitam o tamanho das chaves para confidencialidade, mas não para integridade e autenticação. A SSLv3 permite a realização de conexões não criptografadas, mas autenticadas e protegidas contra ataques deliberados. Isto pode ser útil em lugares onde a criptografia é proibida, como na França. A escolha dos algoritmos e do tamanho da chave é determinada pelo servidor da SSL, mas é limitada pelo servidor e pelo cliente.

b) Eficiência: A criptografia e a decifragem de chave pública são operações demoradas. Em lugar de repetir essa operação a cada comunicação entre um cliente e um servidor, as implementações da SSL podem criar um “segredo mestre”, que é preservado entre as conexões da SSL. Isso permite iniciar conexões seguras desde o princípio, sem a necessidade de se realizar mais operações de chave pública.

c) Autenticações por certificado: A SSL oferece autenticação de cliente e de servidor por meio de certificados digitais. A SSLv3 usa certificados X.509 v3, embora a padronização da SSL pelo IETF (possivelmente chamada de TLS) possa usar tipos de certificados diferentes. A autenticação é opcional, embora certificados de servidor sejam obrigatórios

nas implementações atuais.

d) Flexível em relação aos protocolos: Embora a SSL tenha sido criada para ser executada com o protocolo TCP/IP, na verdade pode ser executada com qualquer protocolo confiável, orientado à conexão, como X.25 ou OSI. Mas não pode ser executado em um protocolo não confiável como o IP *User Datagram Protocol* (UDP – Protocolo de Datagrama de Usuário). Todas as comunicações na SSL acontecem em um único fluxo bidirecional.

O protocolo da SSL foi projetado para oferecer proteção contra ataques de intermediário (man-in-the-middle) e de repetição. Em um ataque de intermediário, um atacante intercepta todas as comunicações entre duas partes, fazendo-as pensar que estão se comunicando. A SSL protege contra ataques de intermediário usando certificados digitais para permitir que o usuário conheça o nome validado do site da Web. Infelizmente, o Netscape Navigator esconde essa informação, tornando-a acessível apenas ao usuário que escolhe o comando "View Document Info (Visualizar Informação do Documento)". Uma interface melhor poderia exibir o nome validado do site da Web na barra de título ou em outro lugar óbvio. A SSL não oferece proteção contra ataques "man-in-the-middle" quando o modo "apenas criptografia" for usado com qualquer tipo de cifragem SSL_DH_anon, pois este modo não permite nem ao servidor, nem ao cliente, autenticarem-se mutuamente.

Em um ataque de repetição, o atacante intercepta as comunicações entre as duas partes e repete as mensagens. Por exemplo, um atacante pode interceptar uma mensagem de um usuário destinada a uma instituição financeira, para que um pagamento seja efetuado; repetindo a mensagem, o atacante poderia fazer com que fossem feitos vários pagamentos, conforme é ilustrado na figura 3.

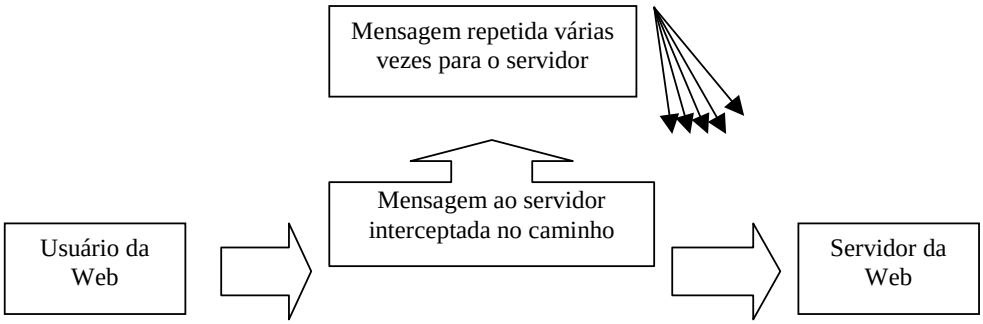

Figura 3 - Ataques de Repetição

a) Suporte para Compactação: em face de os dados criptografados não poderem ser compactados, a SSL oferece a possibilidade de compactá-los antes da criptografia. (No entanto, não há atualmente implementações da SSL que incorporem a compactação).

b) Compatibilidade com SSL 2.0: Servidores com SSLv3.0 podem receber conexões de clientes SSL 2.0 sem forçar o cliente a se reconectar.

As versões de exportação dos programas de SSL podem ser divididas em dois grupos:

a) Chaves públicas para criptografia não podem ultrapassar 512 bits: Versões de exportação da SSL devem usar chaves RSA limitadas a 512 bits. Se um cliente de SSL para exportação conectar-se com um servidor SSL 3.0 que possua apenas uma chave pública RSA de 1024 bits, o servidor criará uma chave pública temporária de 512 bits.

b) Chaves secretas não podem ultrapassar 40 bits: As versões de exportação dos produtos de SSL são mais restringidas, com um tamanho máximo de chave secreta de 40 bits. A SSL usa uma chave criptográfica de 128 bits, mas produz esta chave usando 40 bits de dados secretos. A versão 2.0 envia 88 bits de dados não-criptografados como parte da comunicação. A versão 3.0 produz a chave toda com base nos 40 bits secretos, em conjunto com os dados aleatórios da mensagem SSL Hello. Um atacante determinado poderia decifrar a comunicação testando todas as 2^{40} chaves diferentes.

Em razão de as restrições norte-americanas permitirem a utilização de chaves públicas de 512 bits, mas chaves secretas de apenas 40 bits, muitas pessoas presumem que é tão difícil quebrar uma chave de 512 bits, quanto o é fazê-lo em uma chave de 40 bits. Não é assim. Como a chave de 512 bits é usada repetidamente para criptografar dezenas de milhares de chaves secretas de 40 bits, é razoável que tenha um padrão de segurança mais alto.

Alguns exemplos de implementações da SSL, são: SSL Netscape, SSL Ref, SSLeay e SSL Java.

Presumindo-se que você tenha um servidor de *Web* capaz de realizar a criptografia e que os usuários utilizam um navegador capacitador para SSL, como o *Navigator* ou o *Explorer*, estes podem instruir o navegador a criar uma conexão criptografada pela simples substituição do "http" em seus URLs por "https", escondendo as complexidades da criptografia dos usuários e dos desenvolvedores.

Por exemplo, digamos que você tenha um documento proprietário neste URL:

http://www.company.com/document.html.

Seus usuários podem obter o documento com segurança, neste URL:

https://www.company.com/document.html.

Da mesma forma, se você tiver um formulário CGI, que permite enviar informações de crucial importância (como um número de cartão de crédito), pode-se fazer com que a informação seja enviada na forma criptografada, modificando a condição action= no arquivo HTML, mudando "http" para "https".

Por exemplo, se o rótulo <*form*> de seu arquivo for:

<form method=POST action="http://www.company.com/cgi-bin/enter">, altere-o para

<form method=POST action="https://www.company.com/cgi-bin/enter">.

9 SET

O *Secure Eletronic Transaction* – Transação Eletrônica Segura (SET) é um protocolo criptográfico usado para enviar informações de pagamento pela Internet. O SET foi projetado para criptografar tipos específicos de mensagens relativas a pagamento. Como não pode ser usado para criptografar quaisquer mensagens de texto, os programas que contêm implementações do SET com criptografia poderosa receberam permissão de exportação do Departamento de Estado dos EUA. (Garfinkel, 1999).

O padrão do SET está sendo desenvolvido pela MasterCard, Visa e por várias empresas de computação.

Os objetivos do SET são:

- Oferecer transmissão confidencial.
- Autenticar as partes envolvidas.
- Garantir a integridade dos dados das instruções de pagamento referentes aos pedidos de bens e serviços.
- Autenticar a identidade do portador do cartão e do comerciante.

O SET usa criptografia para as comunicações e assinaturas digitais para autenticação. Com o SET, os comerciantes devem ter certificados digitais oferecidos por seus bancos. Os consumidores também, se desejarem. Durante os testes do SET, a MasterCard exigiu que os consumidores tivessem certificados digitais, e a Visa não.

O sistema SET possui três partes: uma “carteira eletrônica” no computador do usuário; um servidor no site da *Web* do comerciante; e o servidor de pagamento do SET no banco do comerciante. Para usar o sistema, você precisa inserir seu número de cartão de crédito no software da carteira eletrônica. A maioria das implementações irá armazenar o número do cartão de crédito em um arquivo criptografado no disco rígido, ou em um cartão inteligente. O software também cria uma chave pública e uma secreta para criptografar suas informações financeiras antes de enviá-las pela Internet.

Quando você quiser comprar alguma coisa, seu número de cartão de

crédito será criptografado e enviado ao comerciante. O software do comerciante assina digitalmente a mensagem de pagamento e a envia ao banco de processamento, onde o servidor de pagamento decifra todas as informações e executa o débito no cartão de crédito. Por fim, um recibo é enviado ao comerciante e a você, o cliente.

Os bancos que operam com cartão de crédito estão animados com o SET, pois mantém os números dos cartões longe das mãos dos comerciantes. Isso evitaria muitas fraudes, pois são os comerciantes (e seus funcionários) os responsáveis por grande parte das fraudes com cartões de crédito hoje em dia, e não os *hackers* adolescentes. O SET oferece confidencialidade para os números de cartões de crédito, pois são criptografados com o algoritmo RSA, mas não oferece confidencialidade (portanto, nem privacidade) aos outros elementos da transação: esse compromisso teve que ser assumido para que o SET fosse aprovado para a realização de exportações sem que fossem impostas restrições. O SET oferece integridade, autenticação e não-repúdio por meio do uso de funções de codificação de mensagem e assinaturas digitais.

9.1 DOIS CANAIS: UM PARA O COMERCIANTE, OUTRO PARA O BANCO

Em uma transação do SET, há informações que são particulares entre o consumidor e o comerciante (como os ítens pedidos) e também entre o consumidor e o banco (como o número da conta). O SET permite que ambos os tipos de informação digital sejam incluídos numa única transação, por meio de uma estrutura criptográfica chamada assinatura dual. (Gurovits, 1997)

Uma mensagem de requisição de compra dos SET consiste em dois campos, um para o comerciante e outro para seu banco. O campo do comerciante é criptografado com a chave pública do comerciante; o do banco, com a chave pública do banco. O padrão SET não fornece o número do cartão de crédito do consumidor, mas o banco pode, por opção, fornecer o número ao comerciante quando este envia a confirmação. Uma vez que

alguns comerciantes têm sistemas que exigem o número do cartão de crédito, é mais fácil criar este canal no SET em vez dos comerciantes terem que modificar seus sistemas.

Além desses blocos criptografados, a requisição de compra contém codificações de mensagem de cada um dos campos, e uma assinatura. A assinatura é obtida concatenando-se as duas codificações, fazendo a codificação das duas codificações de mensagem, e assinando a codificação de mensagem resultante. A figura 4 mostra como isto é feito. A assinatura dual permite que o comerciante e o banco validem sua assinatura em sua parte da requisição de compra, sem precisar decifrar o campo da outra parte.

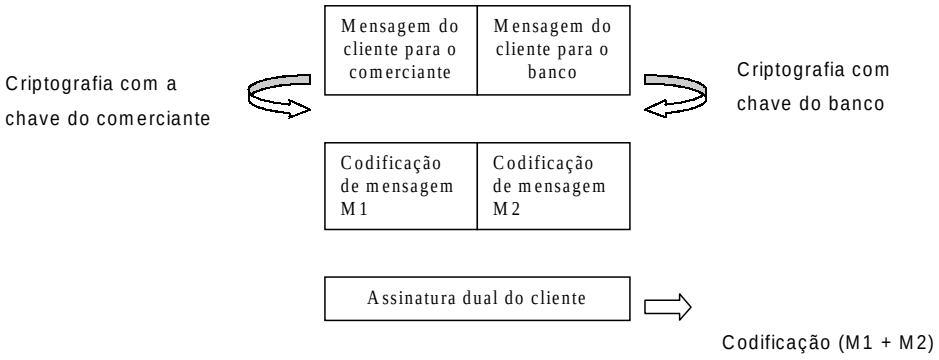

Figura 4 - A Requisição de Compra do SET

10 CONCLUSÃO

A Internet é uma rede de duas vias, sendo ainda a instituição mais democrática do mundo. Talvez uma das mais democráticas da história da humanidade, talvez por não ter dono. Se, por um lado concretiza um sonho secular da humanidade - a globalização - que procurou mercados do Oriente ao Ocidente, hoje chega através da conectividade global ao indivíduo; 0 por outro, facilita as ações criminosas, já que são baseadas quase que essencialmente na inteligência dos criminosos cibernéticos e na facilidade

de se esconderem.

Os negócios e novos mercados estão se direcionando cada vez mais para a Internet e Intranets. Torna-se necessário o conhecimento e a análise dos riscos e vulnerabilidade a que estamos expostos, de forma que possamos definir os mecanismos adequados para a segurança.

Apesar dos problemas, podemos afirmar que o uso adequado da tecnologia de segurança e dos mecanismos de proteção e controle na Internet e Intranet permitem realizar operações comerciais em condições mais seguras do que os meios de transações e comunicações convencionais.

Entretanto, o desconhecimento técnico da segurança, a ausência do foco e disciplina no assunto, além da ausência da adoção de algumas das soluções neste artigo descritas, serão os principais fatores para o aumento dos riscos. Técnicos, executivos e usuários estão diante de um grande desafio.

REFERÊNCIAS BIBLIOGRÁFICAS

AZEVEDO, Luiz Alberto de Oliveira. **Anotações da disciplina Sistemas de Informações Avançados. Curso de Pós Graduação em Desenvolvimento de Aplicações para World Wide Web, UNIDERP**. *Campo Grande/MS, 1999. [não publicado]*

CORRÊA, Nelson. **Análise de Segurança em Interne**t. [S.l.: s.n.], 1999. Disponível em:< http://www.modulo.com.br/noticia/a~anaseg.htm>.

GARFINKEL, Simson; SPAFFORD, Gene. Um Panorama da Segurança na Web, Técnicas de Identificação Digital, Noções Básicas sobre a Criptografia, Criptografia e a Web, Entendendo a SSL e o TLS, Pagamentos Digitais. In: **COMÉRCIO & SEGURANÇA NA WEB**. São Paulo: Market Books do Brasil, 1999. 378 p. ISBN 98-4534 p. 3-24;101-131; 187-250, 313-334.

GUROVITS, Helio. Ilusão de Privacidade. **EXAME**, São Paulo, v.632, p. 135-146. mar 1997.

HOLSCHUH, Henrique. **Pretty Good Privacy**. São Paulo: Unicamp, 1997. Disponível:< http://www.dca.fee.unicamp.br/pgp/pgp/shtml>.

SÊMOLA, Marcos. Já é hora de pensar em e-security. **IDG Now!**, [S.l.: s,n.] 1999. Disponível em: <Internet: http://www.modulo.com.br/noticia/a~esec.htm>.