Sérgio Augusto Carvalho Gomes

Proposta de uma Metodologia para Implementação de Comércio-e Seguro Utilizando o Protocolo TSL.

Monografia de Graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras, como parte das exigências da disciplina Projeto Orientado para obtenção do título de Bacharel em Ciência da Computação.

Orientador
Prof. Bruno Schneider

Lavras
Minas Gerais - Brasil
2002

Sérgio Augusto Carvalho Gomes

Proposta de uma Metodologia para Implementação de Comércio-e Seguro Utilizando o Protocolo TSL.

Monografia de Graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras, como parte das exigências da disciplina Projeto Orientado para obtenção do título de Bacharel em Ciência da Computação.

Aprovada em ____ de _____ de 2002

_____
Prof. André Luiz Zambalde

_____
Prof. Olinda P. Cardoso

_____
Prof. Bruno Schneider
(Orientador)

Lavras
Minas Gerais - Brasil

Ao meu país,
Por tudo que é
E que ainda será!

"Essa terra ainda há
de cumprir seu ideal"

Resumo

Tendo em vista a importância da tecnologia da informação aplicada às organizações através de seus sistemas de informações, e a consolidação da internet como um importante meio de comunicação e negócios na economia atual, este trabalho tem como finalidade propor uma metodologia de implementação de comércio eletrônico seguro baseado nos princípios da segurança da informação e no protocolo TSL (camada de transporte segura).

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

1.1 Apresentação

Atualmente o uso da tecnologia da informação[1] é fundamental para as organizações humanas no mundo inteiro, pois somente através dela é possível automatizar muitos de seus procedimentos e funções, aumentando o controle sobre os recursos, sua flexibilidade e eficiência, garantindo a redução de seus custos operacionais além de outras melhorias importantes [PF00].

Paralela a esta realidade, temos a constante expansão da internet como meio de comunicação e sua consolidação como uma importante ferramenta para expansão dos negócios de uma empresa, através do comércio eletrônico (comércio-e)[2]. Apesar de ser uma modalidade de negócios aplicada ao mercado há mais de duas décadas [Suc99], o comércio-e somente difundiu e deixou de ser um privilégio de grandes corporações, tornando-se acessível para pequenas e médias empresas, através da popularização da internet e o fácil acesso aos equipamentos e tecnologias com a globalização do mercado mundial.

Neste cenário, destaca-se a importância da segurança da informação envolvida nestes sistemas, e o surgimento de ferramentas e técnicas que visam a sua implantação, como o protocolo TSL (camada de transporte segura). Sendo assim, este trabalho apresenta os principais conceitos da segurança da informação e o protocolo TSL, o que conduz a uma proposta de uma

---

[1] Recursos físicos e lógicos utilizados na manIPulação e gerenciamento de informação digital.

[2] Abreviação do termo "comércio eletrônico"

metodologia de implementação de comércio-e seguro utilizando o protocolo TSL, visando criar uma referência para este procedimento.

Capítulo 2

Segurança da Informação em meios eletrônicos

2.1 Introdução

Os sistemas de informação são responsáveis pelo gerenciamento, armazenamento e utilização das informações das organizações humanas, através do uso de um conjunto de recursos físicos e lógicos. Portanto, sua segurança é algo de grande importância para a organização, o que é descrito a seguir por [Fig01]:

'Atualmente as informações contidas em sistemas computacionais são consideradas recursos críticos, tanto para concretização de negócios e tomada de decisões. O que pode acontecer se as informações institucionais caírem nas mãos da concorrência ou fossem corrompidas ou apagadas? Nunca foi tão fácil atacar os sistemas informatizados, já que os sistemas de informação institucionais estão conectados em redes externas.'

A última pesquisa nacional sobre segurança da informação [PNS01], realizada pela empresa Módulo, destaca que 53% das empresas apontam como principal ameaça à segurança da informação os funcionários insatisfeitos. Ou seja, a ameaça de ataque por desconhecidos pela internet, antes apontado por muitos como principal fator de risco à segurança da informação, perde seu destaque para a existência de invasores internos, o que é uma revelação assustadora para muitas organizações que não gerenciam sua segurança interna.

As principais ameaças à segurança da informação segundo [PNS01] são apresentadas na Tabela 2.1:

Funcionário insatisfeito	53%
Acessos indevidos	42%
Vírus	39%
Divulgação indevida	36%
Invasores	33%
Uso de computadores portáteis	30%
Vazamento de informações	30%

Tabela 2.1: Ameaças à segurança da informação

A necessidade da segurança da informação pode ser justificada através da seguinte premissa: Nenhum ser humano é perfeito, sistemas de informação são feitos por seres humanos, logo, nenhum sistema é totalmente perfeito para não haver falhas e totalmente seguros para não serem atingidos.

2.3 Princípios da Segurança da informação

Segundo [MBL00], os princípios da segurança da informação podem ser classificados pela seguinte taxonomia:

Confidencialidade

A informação dever ser somente compreensível para às partes autorizadas. Para garantir este principio utiliza-se a criptografia. Se um método de criptografia é aplicado a uma informação, esta torna-se ilegível, incompreensível para as

pessoas não autorizadas, devido ao fato de desconhecerem qual método ou como este foi utilizado, o que as impede de reverter o processo. Os conceitos de criptografia utilizados neste trabalho são discutidos no Capítulo 3.

Integridade

Considerando que o meio eletrônico por onde passa a informação possa ser acessado por terceiros, é preciso garantir que a informação seja transmitida entre o destinatário e o emissor sem alteração de seu conteúdo. Para tal procedimento, é utilizado um método de código de autenticação da mensagem (CAM). Seu método de funcionamento é apresentado no Capítulo 3.

Autenticidade

Esta é uma questão importante para a segurança da informação, o que levou muitos pesquisadores à procura de soluções para este problema, até que na década de 1970 foi elaborada a criptografia de chave pública, que através do uso de duas chaves, pública e privada, permite garantir a autencidade do documento eletrônico, assim como no mundo real, utiliza-se a assinatura manual para autenticar um documento qualquer. Maiores detalhes sobre o método serão discutidos no próximo capítulo.

Disponibilidade

A segurança da informação deve garantir a disponibilidade da mesma, mesmo que a informação mantenha seu sigilo, integridade e autencidade, ela deve estar disponível para as pessoas autorizadas acessarem. A disponibilidade pode ser garantida através de meios que busquem a segurança ao ambiente onde se encontra a informação, como o Módulo de Segurança da rede, apresentado na seção 2.5 deste capítulo.

2.4 Política de Segurança da Informação

A Política de Segurança da Informação é um conjunto de diretrizes, métodos e procedimentos que regem a gestão da segurança da tecnologia de informação de uma empresa. É um sub-conjunto da política de segurança geral da empresa, que abrange além da segurança dos recursos de tecnologia informação, os recursos humanos e físicos da empresa. Como este trabalho não trata de outras políticas, será utilizado somente o termo política de segurança.

O documento com as políticas de segurança de uma organização deve conter todas as normas, procedimentos e diretrizes da empresa que envolve a segurança das informações da empresa. Todo o conjunto de equipamentos e sistemas lógicos pertencentes à mesma deve ter sua gestão regida por esta política. Por exemplo, qualquer recurso liberado para a utilização dos funcionários, deve existir normas de utilização correta e segura para o mesmo [Set01].

Segundo [Fig01], é importante que a política defina responsabilidades das funções relacionadas à segurança e discrimine as principais ameaças, riscos e impactos envolvidos. A política de segurança deve se integrar às metas de negócio da organização e ao plano de informática. A política de segurança gera impacto em todos projetos de informática, tais como plano, de desenvolvimento de novos sistemas, plano de contingências, planejamento de capacidade, entre outros.

2.4.1 Plano de Contingência

O Plano de Contingência, um importante tópico da política de segurança, é um conjunto de regras e procedimentos para tentativa de recuperação dos recursos do sistema de informação atingidos por um desastre. É um recurso

importante para situações extremas, onde é preciso saber o que fazer para controlar o problema e administrá-lo corretamente.

A importância da elaboração de um plano de contingência para uma organização está em capacitá-la para lidar com situações adversas, amenizando as conseqüências, impedindo que estas levem ao fechamento da organização [Fig01].

2.5 Módulo de segurança da rede

Define-se como módulo de segurança da rede o conjunto de técnicas e ferramentas de segurança utilizadas para implementar as diretivas e procedimentos da política de segurança da informação de uma organização em uma determinada região estratégica de sua rede, responsável por interligar duas ou mais redes, que seja passagem obrigatória e exclusiva para os dados que trafegam entre estas redes.

Através das ferramentas instaladas no módulo de segurança da rede, é possível controlar o acesso aos servidores de serviços, como FTP e HTTP[3], o acesso à rede interna e externa, analisando a origem e o destino dos pacotes, registrando todos os eventos ocorridos, como solicitações de arquivos, conexão e erros, detectar intrusos e tentativas de invasões, descobrir falhas de segurança, além de outros recursos. É importante que este sistema seja bem estruturado e configurado, pois devido a sua posição estratégica na rede, pode causar problemas de conexão e trafego. Na figura 2.1 é ilustrado um exemplo de módulo de segurança.

[3] FTP: Protocolo de transferência de arquivos
HTTP: Protocolo de transferência de arquivos hiper-texto (páginas HTML em geral)

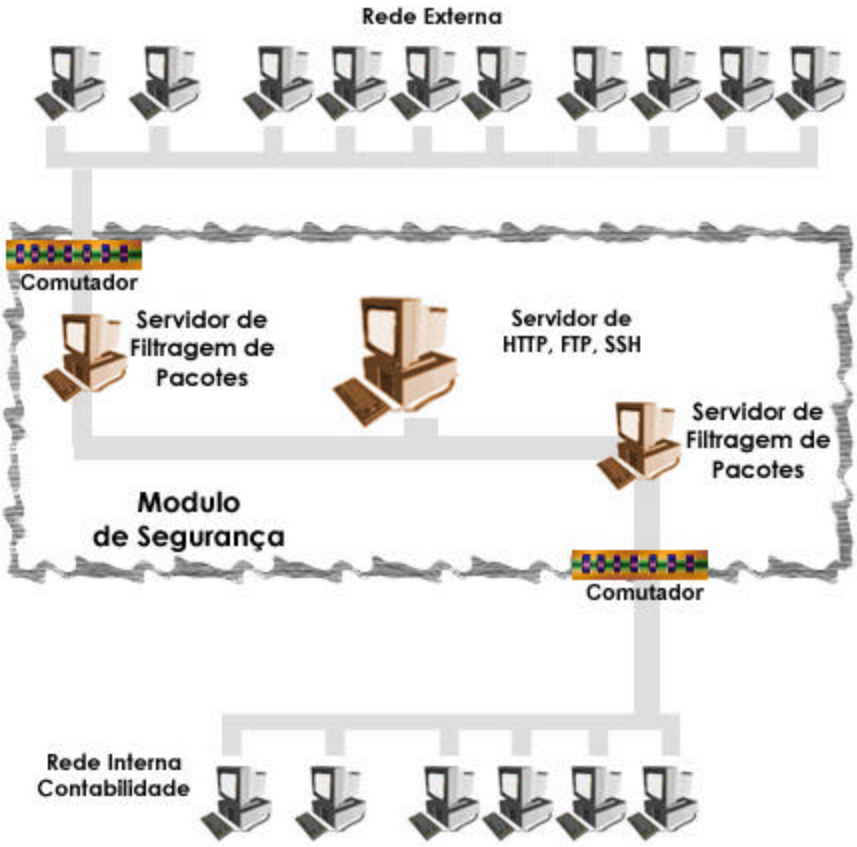


Figura 2.1: Exemplo de um módulo de segurança

2.6 Soluções e ferramentas de segurança

Existem diversas técnicas e ferramentas de segurança que podem ser utilizadas em um sistema de segurança, como o controle de acessos de usuários, cópias de segurança e arquivos de registro. Neste capítulo são apresentadas e descritas as principais ferramentas de segurança de rede da atualidade, o que

torna necessário apresentar ao leitor os conceitos básicos sobre quadros e pacotes de dados.

2.6.1 Quadros e Pacotes de Dados

Para as ferramentas de segurança de rede, os principais objetos de trabalho são o quadro e pacote de dados, duas estruturas de dados do modelo de referência TCP/IP. O modelo TCP/IP é um conjunto de especificações que define um protocolo de comunicação entre computadores, definido como protocolo padrão da Internet. Na Figura 2.2, é ilustrado o modelo de referência TCP/IP, com suas respectivas camadas onde se encontram os quadros e pacotes:

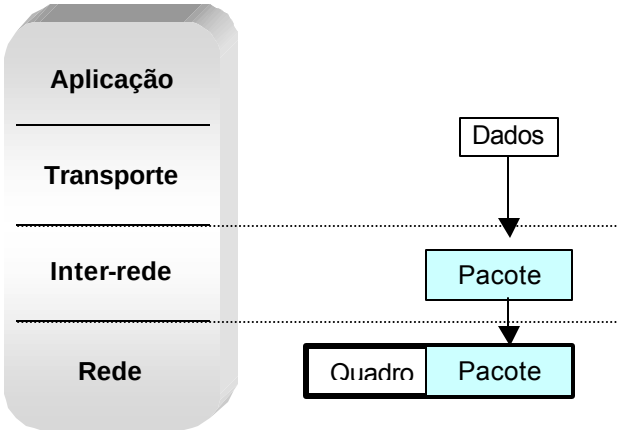


Figura 2.2 - Modelo de Referência TCP/IP e suas estruturas de dados

Considerando que a camada de Aplicação é a camada mais próxima do usuário e a camada de Rede fica entre a máquina e o meio físico de comunicação, a Figura 2.2 ilustra como os dados do usuário são passados para a camada de Inter-rede e guardados no pacote, e em seguida o pacote é passado para a camada de Rede e guardado dentro de um quadro. Este processo de armazenar

os dados da camada anterior na estrutura de dados da camada presente pode ser denominada de encapsulamento.

O pacote contém os dados da camada anterior, além de outros dados importantes, como o número IP de origem e destino, o que é ilustrado na Figura 2.3:

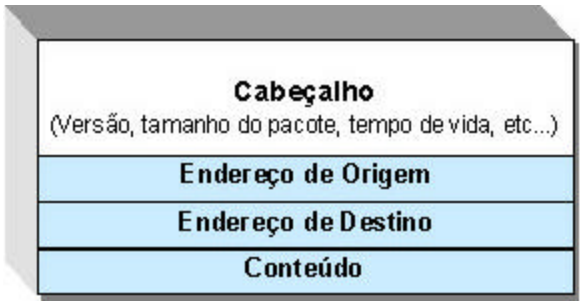


Figura 2.3: Estrutura do pacote de dados

Assim como o pacote, o quadro possui um campo responsável pelo armazenamento dos dados da camada anterior, além dos endereços de origem e destino, que armazenam o número MAC, um número de identificação da placa de rede, que indica qual máquina da rede deve receber o quadro.

Na próxima seção, será descrito o funcionamento das principais ferramentas de segurança da rede e como utilizam as informações dos quadros e pacotes.

2.6.2 Filtro de pacotes

Conhecido popularmente como "firewall", uma alusão aos muros de alvenaria construídos entre prédios de madeira para evitar a propagação do fogo, devido à sua característica de impedir a entrada de pacotes não autorizados,

protegendo a rede de pacotes suspeitos [TAN97]. São sistemas ou equipamentos que possuem uma ou mais interfaces de rede, com a capacidade de analisar todos os pacotes que entram ou saem para a rede quanto a sua origem, destino, serviço de rede solicitado e conteúdo.

A filtragem de pacotes é uma importante ferramenta de segurança em redes, mas seu desempenho depende de sua configuração correta. Atualmente, existem três modelos padrões para filtros de pacotes, descritos a seguir:

- **Filtro de pacotes básico**: Possui a capacidade de analisar diversos campos do cabeçário do pacote de dados, como origem, destino, tipo de serviço e outros.
- **Filtro de pacotes a nível de aplicação**: Possui a capacidade de analisar o campo de dados do pacote de dados, podendo restringir a passagem de determinados conteúdos considerados indesejáveis.
- **Filtro de pacotes híbrido**: Possui ambas capacidades dos modelos acima em uma só maquina.

2.6.3 Sistema de detecção de intrusos (SDI)

São sistemas que analisam o tráfego da rede através dos pacotes, verificando o conteúdo a procura de dados suspeitos que possam indicar uma tentativa de invasão. O sistema de detecção de intrusos possui um módulo responsável por capturar os pacotes que chegam a sua interface de rede que opera no modo promíscuo, ou seja, este módulo "escuta" todo o tráfego que passa por aquele segmento de rede. Após a captura dos pacotes, um outro módulo do sistema analisa estas informações baseado num arquivo de regras definidos pelo administrador do sistema. Este arquivo de regras contem as "assinaturas" e ações, que definem padrões para reconhecimento de tentativas de ataque ou procedimentos ilícitos. Quando o SDI reconhece alguma irregularidade, ele pode

simplesmente relatar o fato para o administrador através do correio-e[4] ou até tomar medidas para impedir o ataque, como encerramento da conexão.

2.6.4 Analisadores de rede

São ferramentas que automatizam o processo de checagem de falhas de segurança. Estes sistemas analisam os computadores ligados à rede e verificam quais os serviços ativos e as portas abertas. Após esta analise, o sistema retorna um relatório contendo possíveis falhas na segurança, como portas abertas, serviços ativos desnecessários ou mal configurados e falhas conhecidas em determinados programas. Seu uso é importante para verificar a segurança da rede em seu desenvolvimento e manutenção.

2.6.5 Roteadores e comutadores

Assim como uma pessoa precisa se dirigir a um aeroporto e apresentar seu passaporte para viajar para outros países, os pacotes e quadros[5] precisam passar pelos roteadores e comutadores para alcançarem outras redes.

Os roteadores funcionam na camada de inter-rede do protocolo TCP/IP, ilustrado na figura 2.3, baseados no número IP de destino e origem. Constitui um recurso básico de segurança, que impede que uma rede seja sobrecarregada de pacotes indesejados vindos da Internet, ou impedir a saída dos pacotes que devem trafegar internamente, por exemplo.

Os comutadores atuam na camada de rede do protocolo TCP/IP, baseado no endereço MAC. Seu funcionamento se baseia em decidir para onde enviar o

[4] Abreviatura de correio eletrônico

quadro, baseado no endereço MAC, na rede de origem e na tabela de regras. Contribui consideravelmente para a segurança da rede, pois pessoas mal intencionadas podem configurar suas placas de rede para operarem no modo promíscuo, permitindo que a máquina receba todos os quadros que passam pela sua interface, quando deveria receber somente os que contêm seu endereço MAC. Utilizando o comutador, a rede pode ser segmentada em diversas sub-redes, assim estas placas que operam no modo promiscuo só "escutam" os quadros que circulam pelo seu segmento, pois os comutadores só permitem a passagem de um quadro para seu segmento correspondente.

Capítulo 3

Criptografia

Este capítulo tem a finalidade de apresentar os conceitos de criptografia utilizados pelo protocolo TSL.

3.1 Criptografia Assimétrica

A característica fundamental desta modalidade de criptografia é o uso de chaves distintas durante o processo de criptografia, onde por exemplo, a chave usada pelo emissor para cifrar a informação não é a mesma usada pelo receptor para decifrar a mensagem. Existem diversos métodos que implementam a criptografia assimétrica, como o método da Mochila e de Rabin [Raul95] por exemplo, mas o mais conhecido é a criptografia de chave pública, baseado no uso de um par de chaves distintas, a pública e a privada, para cada parte envolvida no processo de comunicação segura, o que é discutido a seguir.

3.1.1 Criptografia de Chave Pública

O Conceito de Criptografia de Chave Publica foi desenvolvido na década de 1970 com o objetivo de desenvolver um método de criptografia que resolvesse três problemas pertinentes à criptografia simétrica[6] [TAN97]:

-Troca de chaves em meios inseguros

Ao transmitir uma mensagem cifrada utilizando a criptografia simétrica, é necessário que a outra parte tenha a mesma chave. Caso este não possua a chave, será preciso enviar a chave para que o receptor possa decifrar a mensagem.

[6] Método de criptografia que utiliza somente uma chave em seu funcionamento

-Autencidade do Emissor da Mensagem

Como garantir a autencidade num meio eletrônico de acesso público como a Internet? É até possível, através da criptografia simétrica, implementar um sistema onde as partes podem se autenticar, mas este sistema seria restrito a um numero pequeno de participantes devido à algumas restrições, como a necessidade de cadastro geral de todas as partes envolvidas, o que seria inviável para meios de comunicação como a Internet.

-Gerenciamento das chaves

Uma determinada empresa resolve trocar mensagens confidenciais com outras empresas utilizando chaves secretas. Para isto, é criada uma nova chave para cada empresa que ela se comunica, e esta chave ficará em posse das duas empresas. Este sistema pode até funcionar bem entre dez ou vinte empresas. O problema é que quanto maior o número de participantes, maior será a complexidade em seu gerenciamento, o que torna este procedimento inviável.

A criptografia de chave pública resolve estes e outros problemas através do uso de um par de chaves, pública e privada, o que permite o uso de assinaturas digitais e uso de certificados emitidos por uma Autoridade Certificadora, apresentados nas seções 3.2 e 3.3.

3.1.2 Funcionamento

A base da Criptografia de Chaves Públicas consiste na utilização de duas chaves para cada entidade participante; uma chave privada e outra pública. Existe uma relação importante entre estas duas chaves: Se uma mensagem é criptografada com a chave pública, só pode ser decifrada pela chave privada

correspondente, e for cifrada pela chave privada, poderá ser decifrada pela chave pública [Fig01]. Estes princípios podem ser definidos nas três regras a seguir, e um exemplo de funcionamento é ilustrado na Figura 3.1:

1 - Cpr(Cpu(M)) = M

2 - Cpu(Cpr(M)) = M

3 - É excessivamente difícil deduzir Cpr de Cpu

Onde; Cpr = Chave privada; Cpu = Chave pública; M = Mensagem

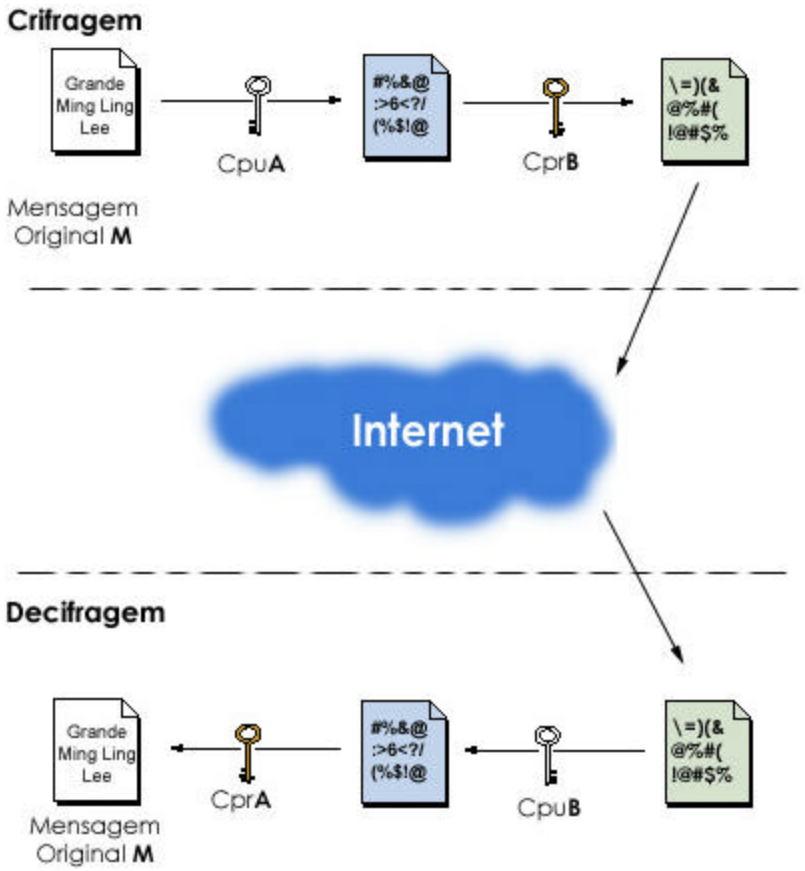


Figura 3.1 - Exemplo do funcionamento da criptografia de chave pública

3.2 Assinatura digital

Com o uso do par de chaves publica e privada, é possível implementar o conceito de assinatura digital. A assinatura digital é o resultado da aplicação da chave privada a uma mensagem, pois, quem possuir a chave pública correspondente e conseguir decifrar a mensagem, terá certeza da autencidade do emissor. Este modelo garante a autencidade, mas não a privacidade total da mensagem [Rau95].

3.3 Autoridade Certificadora e Certificados

O uso da assinatura digital foi um fator importante para a consolidação da segurança nos meios eletrônicos de comunicação. Mas somente a aplicação de sua técnica, descrita na seção anterior, não é suficiente para garantir a veracidade e autoria como um documento autenticado em cartório, por exemplo. Se não existe nenhuma entidade responsável por certificar a posse da assinatura digital, não há garantias na utilização desta.

Com a finalidade de transportar para o mundo digital as funções dos cartórios e autoridades emissoras de documentos, capazes de certificar a vontade humana representada em documentos físicos, foram criados os conceitos de autoridades certificadoras e certificados digitais, definidos a seguir.

A Autoridade Certificadora (AC) deve ser uma entidade idônea, registrada em cartório real e regulamentada por uma política de funcionamento e segurança. Ela é responsável por emitir certificados autenticando as assinaturas digitais de pessoas físicas e jurídicas. Todos certificados emitidos por ela são de sua responsabilidade, por isto ela deve exigir cadastro completo de seus usuários e que eles assinem termos de compromisso, evitando emitir certificados para pessoas ou empresas que não pretendem seguir sua política de uso.

O certificado digital é um documento digital que contém diversas informações sobre o proprietário, assim como uma carteira de identidade. Suas características são citadas e comparadas na Tabela 3.1:

Item	Carteira Identidade	Certificado Digital (Padrão X509 v3[7])
Conteúdo	-Nome -Filiação -Código de pessoa física -Código da identidade -Órgão expedidor -Impressão digital -Fotografia	-Versão do certificado; -Emissor: nome da Autoridade Certificadora; -Validade: data de geração e de expiração do certificado; -Assinatura: algoritmo utilizado pela AC para assinar o certificado; -Usuário: entidade associada com a chave pública; -Informação da Chave Pública do Usuário -Número Serial: número do certificado (identificação única dentro de uma AC)
Certificação do Titular	Exame da impressão digital e reconhecimento pela foto	Chave pública do portador, para verificar a autencidade de sua assinatura digital; registro em uma autoridade certificadora
Certificação do Emissor	Documento em papel oficial timbrado, registro do documento em um órgão responsável reconhecido pelo governo	Chave pública da autoridade, para confirmar a autencidade de sua assinatura digital; registro da autoridade certificadora por uma entidade responsável pelo seu funcionamento.

Tabela 3.1: Características do certificado digital

[7] Padrão de certificado digital criado pela União Internacional de Telecomunicações

3.4 Código de autenticação de Mensagem (CAM)

Sua finalidade é garantir a integridade da mensagem. Aplicando-se um método de CAM à uma mensagem, é obtido uma seqüência de caracteres exclusiva, como a impressão digital de uma pessoa, a possibilidade de duas mensagens gerarem uma mesma seqüência é remota, praticamente impossível [Rau95]. Além disto, a partir deste código de autenticação gerado não é possível obter a mensagem original novamente, este serve somente para verificar a autencidade da mensagem original.

3.5 Infra-Estrutura de Chave Pública Brasileira - ICP-Brasil

Em 27 de julho de 2001, a Medida Provisória 2.200-1 instituiu a ICP-Brasil, que possibilita a habilitação de instituições públicas e entidades privadas para atuarem na validação jurídica de documentos produzidos, transmitidos ou obtidos sob a forma eletrônica. Com essa medida passa-se a dispor de alternativa para realizar eletronicamente transações que até então não se podiam fazer e exigiam registros em papel escrito para adquirirem validade [TEM00]. Para regulamentação e gerenciamento da ICP-Brasil, foi criado pelo governo o seu comitê Gestor, responsável pela Autoridade Certificadora Raiz, que é a autoridade máxima de certificação.

O modelo da ICP-Brasil segue normas de padrões internacionais, além de métodos e procedimentos desenvolvidos em outras experiências do governo, quando em 2000 havia desenvolvido uma ICP própria para órgãos e entidades de Administração Publica Federal. Apesar de todo esforço do governo, a ICP-Brasil ainda precisa sofrer algumas pequenas modificações, segundo [Rez01], seu sistema de distribuição de certificados e gerenciamento de datação das chaves

ainda não foram totalmente especificados. Para maiores informações, os regulamentos e serviços estão disponíveis no sítio: http://www.icpbrasil.gov.br

Capítulo 4

O Protocolo TSL

4.1 Introdução

O Protocolo TSL (Camada de transporte segura), foi desenvolvido pela IETF (Força Tarefa de Engenharia para Internet) em 1999 baseado no protocolo SSL (Camada de conexão segura) 3.0 da empresa Netscape Communications. O TSL tem como finalidade prover comunicação segura pela internet, utilizando métodos de criptografia simétrica e assimétrica. Neste capitulo serão descritos os objetivos deste protocolo, alem dos princípios de seu funcionamento.

Conforme descrito em [DA99], os objetivos do TSL, em ordem de prioridade, são:

1 - Garantir o sigilo e a segurança dos dados de uma conexão entre duas partes através do uso de criptografia.

2 - Permitir que programadores possam desenvolver aplicações utilizando TSL independente de sua plataforma de trabalho, garantindo a sua interoperabilidade.

3 - Prover uma estrutura adequada para incorporar novos métodos de criptografia e chave pública quando necessário, sem a necessidade de criar um novo protocolo ou uma nova biblioteca de segurança inteira, garantindo assim a extensibilidade no protocolo.

4 - Disponibilização de um esquema opcional para armazenamento temporário de dados das sessões estabelecidas, o que ajuda a diminuir o trafego entre as partes, o que implica num melhor desempenho do funcionamento do protocolo.

4.2 Exemplo de funcionamento do protocolo TSL

Para ter uma visão geral do funcionamento do protocolo TSL, será descrito de uma maneira simples e resumida, como é um procedimento para estabelecimento de uma conexão segura entre um cliente e um servidor.

1- O cliente faz uma requisição ao servidor para estabelecer uma conexão segura via TSL
2- O servidor envia seu certificado contendo sua chave pública ao cliente.
3- O cliente pode reconhecer ou não a legitimidade do certificado do servidor, caso aceite, o processo continua
4- O cliente cria uma chave secreta aleatória, cifra esta com a chave pública do servidor e a envia.
5- O servidor, usando a sua chave privada, consegue a chave secreta.
6- Cliente e servidor começam a se comunicar cifrando/decifrando as mensagens com a chave secreta, utilizando um algoritmo de criptografia simétrico, durante toda a existência da conexão segura.

É considerado que ambos as partes possuam o protocolo TSL instalado em suas máquinas, o qual já é encontrado nos navegadores mais populares da internet como Netscape e Internet Explorer, além de sua versão para servidor, disponível para os principais servidores HTTP do mercado.

A seguir, serão apresentados com mais detalhes, os principais conceitos, os procedimentos e processos existentes no protocolo TSL.

4.3 Conceitos

Funcionando na camada de transporte do modelo de referencia TCP/IP, conforme ilustrado na Figura 4.1, o protocolo TSL interage com a camada de

aplicação, por onde passam as informações a serem cifradas ou decifradas, e com algum protocolo de transporte seguro, como o TCP, que é utilizado para enviar e receber os dados cifrados.

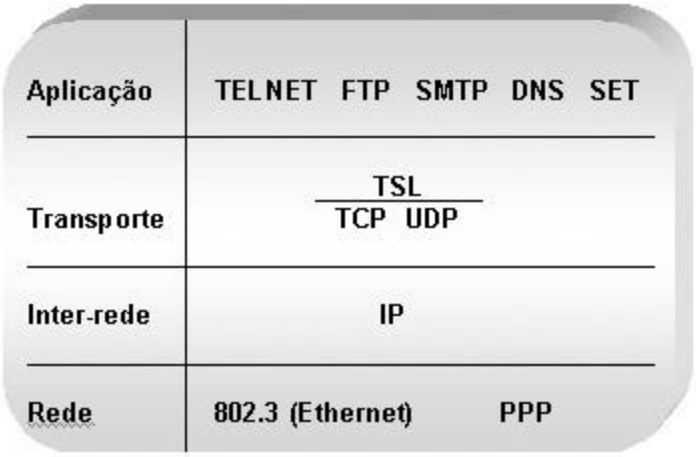
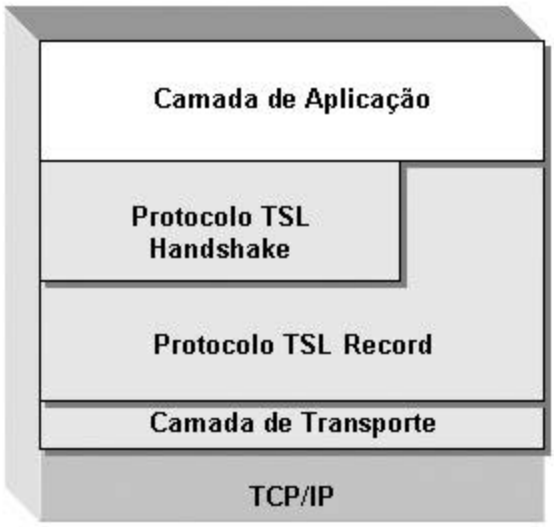


Figura 4.1: Camada de atuação do TSL

O protocolo TSL é constituído de duas camadas, sendo que uma delas contém o protocolo TSL Record e na outra se encontra o protocolo TSL Handshake, como demonstrado na Figura 4.2. A camada que contém o protocolo TSL Handshake interage com a camada de aplicação, sendo responsável pela autenticação das partes e negociação de parâmetros iniciais. A camada inferior, que interage com um protocolo de transporte seguro, contém o protocolo TSL Record, responsável pela criptografia, encapsulamento e compactação dos dados após o estabelecimento de uma conexão segura.



Fgura 4.2: Estrutura do TSL

-Protocolo TSL Handshake

A parte inicial do funcionamento do protocolo TSL é a execução do protocolo TSL Handshake. Este protocolo é responsável por estabelecer parâmetros de segurança para o protocolo TSL Record, autenticação das partes e reportar possíveis erros. Através destes procedimentos, o protocolo pode estabelecer uma sessão, que é uma conexão segura estabelecida entre duas partes. A sessão é definida pelos seguintes parâmetros [DA99]:

- Identificador de sessão (session identifier):
Uma seqüência de bytes arbitrária definida pelo servidor para identificar uma sessão ativa
- Certificado (peer certificate):
Contém o certificado de uma entidade no padrão X509v3, nele se encontra sua chave pública além de outras informações sobre a sua identificação e autoridade certificadora.

- Método de compressão (compression method):
O algoritmo usado para comprimir dados antes de criptografá-los.
- Especificação de criptosistemas (cipher spec):
Especifica quais algoritmos de criptografia (DES, IDEA) e autenticação de mensagens (MD5, SHA) serão usados.
- Chave mestre (master secret):
Chave secreta de 48 bytes compartilhada entre o cliente e servidor.
- Resumível (is resumable):
Um sinal que indica quando a sessão pode ser usado para novas conexões.

O protocolo TSL Handshake, além destes módulos apresentados, é constituído por dois protocolos internos: O protocolo de Especificação de Mudança de Cifra (change cipher specification protocol) e o protocolo de Alerta (Alert protocol).

O protocolo de Especificação de Mudança de Cifra tem como finalidade indicar alguma mudança no uso dos criptosistemas definidos durante a negociação. O protocolo consiste em uma simples mensagem, armazenada na variável **change_cipher_spec**, que indica para as partes participantes qual método de criptografia deve ser utilizado naquele momento.

O protocolo de Alerta é responsável pelo tratamento de erro do protocolo TSL. Quando ocorre qualquer erro é enviada uma mensagem de alerta para o outro lado da conexão. Dependendo do nível do erro a conexão é abortada.

O Protocolo Handshake é a principal parte do TSL. Ele é constituído por duas fases. Na primeira, é feita a escolha da chave entre o cliente e o servidor, a autenticação do servidor e a troca da chave *Master*. Já na segunda, é feita a autenticação do cliente (se requerida) e o fim do *handshake*. As mensagens trocadas durante as negociações do protocolo TSL Handshake seguem o formato da Tabela 4.1, onde:
- HandshakeType: indica o tipo de mensagem de *handshake* sendo enviada

- Tamanho: tamanho do corpo em bytes
- Corpo: Os dados da mensagem

HandshakeType	Tamanho	Corpo

Tabela 4.1: Formato da mensagem do protocolo TSL Handshake

-Protocolo TSL Record

Este protocolo é responsável pela rotina de funcionamento após o estabelecimento da conexão. Basicamente, ele envolve procedimentos para receber e enviar dados, fragmentar mensagens em blocos manipuláveis, comprimir ou não os dados, aplicar um código de autenticação da mensagem (CAM), criptografar e decifrar as mensagens. A Figura 4.3 ilustra estes procedimentos num fluxograma:

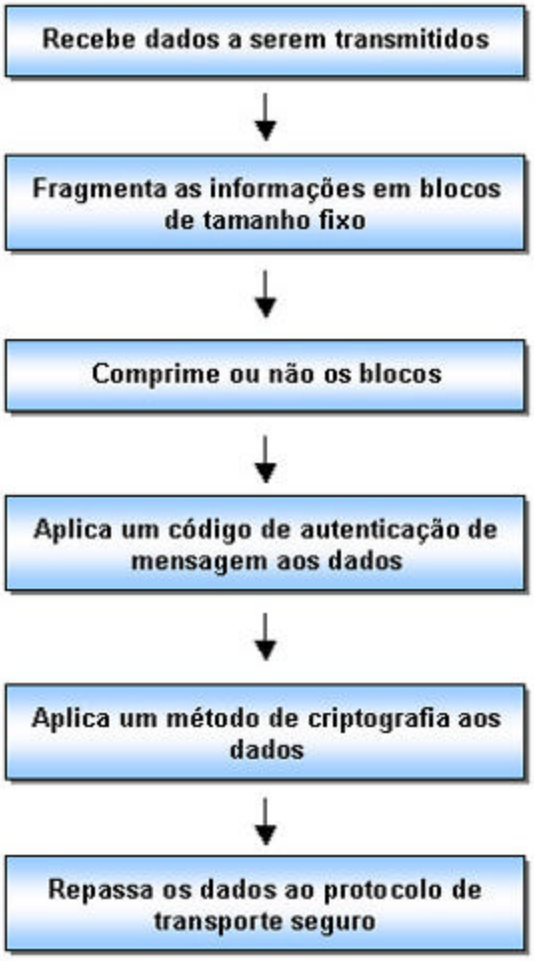


Figura 4.3: Fluxograma do protocolo TSL Record

Analisando a figura acima, é possível descrever o caminho percorrido pelos dados ao passar pelo protocolo. Inicialmente, o protocolo recebe os dados da camada superior, depois são divididos em blocos de tamanho fixo que podem ou não serem comprimidos, é aplicado um método de autenticação de mensagem (CAM), como o MD5 ou SHA, e finalmente é aplicado um método de

criptografia simétrico, agora os dados estão protegidos e podem ser repassados para a outra parte através do protocolo de transporte.

O caminho reverso, ou seja, quando os dados chegam na outra parte, segue os mesmos procedimentos descritos acima numa seqüência inversa. O protocolo de transporte da maquina recebe os dados cifrados e os repassa ao protocolo TSL. Primeiramente os dados são decifrados, aplicado-se o mesmo método e a chave secreta desta sessão. Assim, será possível aplicar um método de código de autenticação de mensagem (CAM) aos dados, e se o resultado deste método coincidir com o código que chegou com a mensagem, a integridade desta é confirmada. Agora, a informação original será recomposta seguindo o caminho inverso da fragmentação, e assim poderá ser apresentada à camada de aplicação.

4.4 Criptosistemas utilizados

Defini-se quatro grupos para representar o conjunto de algoritmos criptográficos utilizados pelo protocolo TSL, conforme citado abaixo [DA99]:

- Algoritmos simétricos: estes algoritmos são utilizados no sigilo dos dados trafegados durante uma sessão TSL. Na atual especificação do TSL são usados os algoritmos RC4, DES, 3DES, RC2 e IDEA .

- Algoritmos assimétricos e de derivação de chaves: algoritmos utilizados para a troca de chaves e para o processo de assinatura digital. Neste grupo estão o RSA, o DSA (somente assinatura) e o Diffie-Hellman (derivação de chaves).

- Algoritmos de compilação: usados para prover a integridade das mensagens enviadas e no processo de criação dos segredos. São especificados o MD5 e o SHA.

- Algoritmos de compactação: na atual versão do TSL não há nenhuma especificação para funções de compactação.

4.5 Conclusões sobre o protocolo TSL

O protocolo TSL apresenta muitas vantagens, sendo:

- Protocolo independente de aplicações, usado em diversas aplicações baseadas em HTTP, FTP, SMTP, Telnet e SET.
- Compatível e similar com o protocolo SSL 3.0.
- Suporta o uso do algoritmo de criptografia de Curva Elíptica.
- É flexível e de fácil manutenção, podendo se adaptar a novos métodos de criptografia

O protocolo por si só não garante a segurança, pois somente o uso da criptografia não satisfaz todos os princípios da segurança da informação. O protocolo pode estabelecer vários níveis de segurança, de acordo com a sua configuração e do ambiente onde será executado, visto que o servidor com falhas de segurança pode afetar o funcionamento do protocolo. Na configuração do protocolo podem ser estabelecida regras como tamanho das chaves, autoridades certificadoras confiáveis e qual nível de autenticação a ser adotado: nenhuma autenticação, autenticação de ambas as partes ou autenticação somente do servidor.

Capítulo 5

A Metodologia

5.1 Introdução

Baseado nos princípios apresentados nos capítulos anteriores e no paradigma de engenharia de sistemas de informação denominado Ciclo de Vida Clássico, foi elaborada uma metodologia para implementação de um sistema de comércio-e seguro utilizando o protocolo TSL.

O paradigma "Ciclo de Vida Clássico" ou "Cascata" é um conjunto de etapas contendo procedimentos para uso de métodos e ferramentas de engenharia, com a finalidade de definir meios para o desenvolvimento de um sistema de informação de uma forma metódica e eficiente [Pres95]. Este paradigma requer uma abordagem sistemática, seqüencial no desenvolvimento do sistema, iniciando ao nível de sistema e avança ao longo da análise, projeto, codificação, teste e manutenção, resumindo, para começar uma nova fase é preciso que a presente esteja completa. Desta forma, esta metodologia objetiva a implementação de sistemas de comércio-e baseados em modelos bem definidos, onde seja possível completar cada fase em suas tarefas para seguir adiante.

Sendo assim, a metodologia encontra-se divida em 6 fases: Análise e Planejamento, Projeto, Implementação, Testes, Disponibilização e Manutenção. As fases funcionam num sistema linear, onde a saída de uma é a entrada da próxima, como demonstrado na Figura 5.1. Esta metodologia é de âmbito geral, o que significa que cada organização deve adaptá-la de acordo com suas características e necessidades.

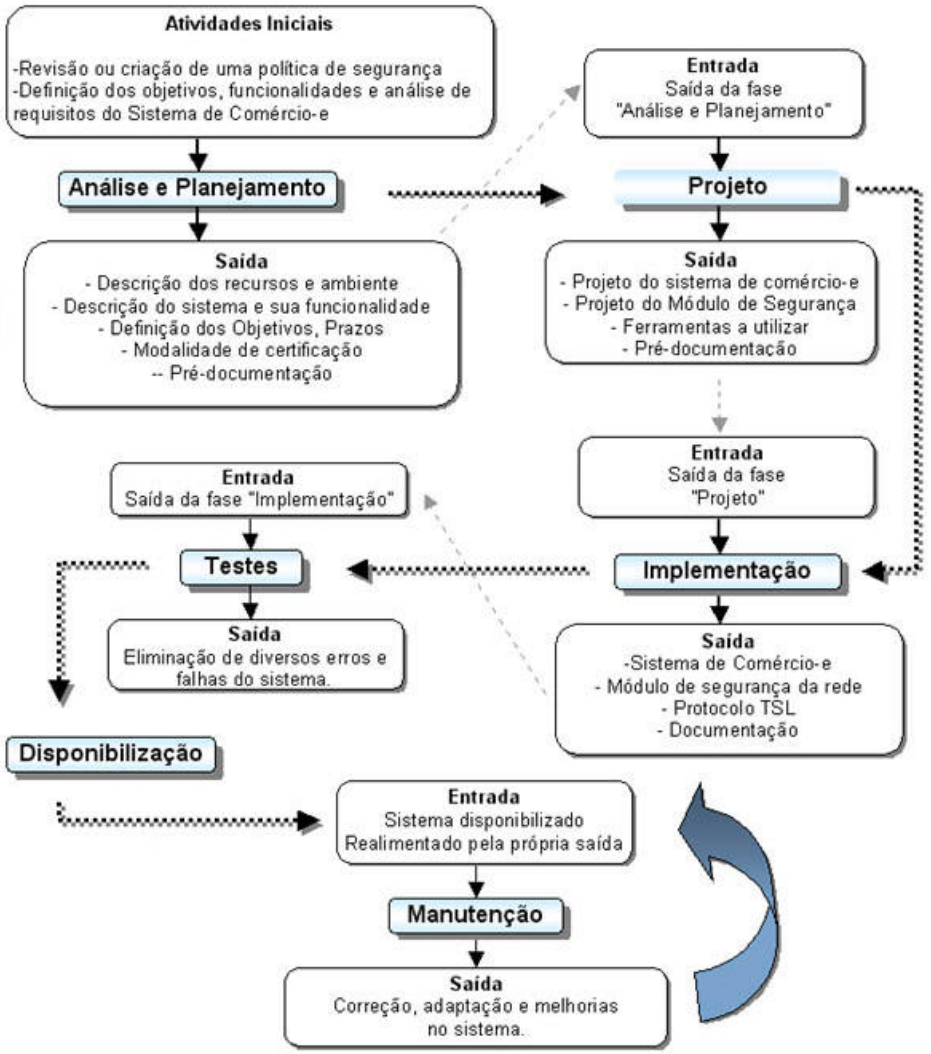


Figura 5.1: Fluxograma da metodologia

5.2 Fase 1: Análise e Planejamento

5.2.1 Etapa 1- Revisão ou criação da política de segurança da Empresa

Inicialmente, é considerado que o responsável pela análise e planejamento tenha conhecimentos sobre o funcionamento, organização e a estratégia geral da empresa, o que é fundamental para a realização de um projeto abrangente e funcional. Esta etapa é responsável pela criação ou revisão da política de segurança de informação da empresa. Caso esta já exista e atenda às necessidades da empresa, prossiga para a Etapa 2.

Nesta etapa, o responsável deve levantar informações acerca dos seguintes itens:

- Recursos disponíveis (Equipamentos e Sistemas computacionais) e a forma como são utilizados.
- Recursos Críticos (recursos necessários para garantir o funcionamento básico da organização).
- Análise de Riscos e Impactos.
- Classificação das informações.
- Propriedade das informações e recursos computacionais.
- Objetivos de segurança.

Estes itens e mais algumas particularidades da empresa, relacionadas à sua segurança, serão responsáveis pela elaboração do documento que servirá de base para a política de segurança, além de informações importantes também para a própria organização, como:

- O que deve ser protegido, quais as ameaças mais prováveis, qual relevância disto para a organização?

- Como é praticado a segurança atualmente?

- Qual impacto na organização caso haja falhas de segurança no seu sistema de informação?

- Qual expectativa da alta direção, dos funcionários e clientes em relação á segurança da informação?

Baseado neste documento e numa norma padrão como a NBR 17799:2001[8], é possível revisar ou mesmo elaborar uma nova política de segurança da informação para empresa [ABNT01]. É importante ressaltar que dentro desta política de segurança deve existir um plano de contingência, um quesito imprescindível da política de segurança para situações inesperadas e críticas. Além disto, esta política deve estar em conformidade com as metas de negócio e a política de segurança geral da organização, o que garante o emprego correto deste importante recurso.

5.2.2 Etapa 2 - Análise de requisitos do Sistema de Comércio-e

Quando uma empresa deseja fazer uso da Internet como ferramenta de negócios, é preciso definir quais serão os objetivos, funções, avaliar seus recursos disponíveis, analisar os requisitos e riscos pertinentes e outros fatores de decisão. Esta etapa especifica um método para levantar informações necessárias para projetar e modelar o sistema de comércio-e desejado.

Entrada:

- Objetivos do sistema.

[8] Norma da ABNT que define diretivas de segurança da informação.

Definir em qual modalidade de negócios se enquadra:

- Negócios para clientes
- Negócios para negócios

- Quais produtos ou serviços serão disponibilizados.
- Análise dos requisitos (função, desempenho e interface desejados).
- Recursos disponíveis (Sistemas de informação, equipamentos, topologia da rede)
- Análise dos riscos (identificação, projeção e avaliação dos possíveis riscos e ameaças).
- Segurança desejada.
- Qual modelo de certificação e autenticação será utilizado.

Saída:

- Definição dos objetivos.
- Especificação dos requisitos necessários e funcionamento geral do sistema.
- Especificação dos recursos de segurança a serem utilizados.
- Definição do orçamento e prazos a serem cumpridos.
- Pré-documentação do sistema.

5.3 Fase 2 - Projeto

A partir das informações devidamente elaboradas na fase 1, será possível prosseguir com o desenvolvimento do sistema, iniciando seu projeto. A fase de projeto inicia o trabalho de detalhamento do sistema, com a especificação da arquitetura do sistema, procedimentos e funções, interface e estrutura de dados. Esta representação do sistema permite que este seja avaliado antes de ser

implementado, adequando e corrigindo de acordo com as necessidades e requisitos previstos. Além disto, o projeto do sistema constituirá uma importante parte da documentação do sistema.

Entrada:

Resultado da saída da fase anterior.

Saída:

Através do uso de uma linguagem de modelagem, como a UML, obtém-se:

-Representação dos casos de uso do sistema de comércio-e, suas entidades e relacionamentos.

-Representação das entidades e relacionamentos do módulo de segurança.

-Pré-documentação.

-Especificação das ferramentas a serem utilizadas:

- Sistema operacional dos servidores.
- Servidor HTTP.
- Ferramenta TSL.
- Ferramentas do módulo de segurança (filtro de pacotes, SDI, analisador de redes e outros).

5.4 Fase 3 - Implementação

A fase seguinte após o projeto é a implementação do sistema, baseada na saída da fase anterior e nas especificações da política de segurança , conforme descrito abaixo:

5.4.1 Etapa 1 - Preparação do ambiente

1)Módulo de segurança

-Instalação dos roteadores, comutadores e repetidores.

-Instalação de servidores e/ou equipamentos das ferramentas de segurança nos pontos estratégicos da rede, onde a passagem do fluxo de dados da rede seja obrigatória.

-Instalação das ferramentas (filtros de pacotes, SDI, analisadores e outros).

2)Sistema de Comércio-e

-Implementação do sistema de comércio-e. Sua interface é definida através da linguagem HTML, podendo utilizar de linguagens de programação para definir suas funcionalidades, interação com banco de dados e outros sistemas.

-Instalação de um servidor de rede para o sistema de comércio-e.

a)Instalação do servidor HTTP

b)Instalação do sistema de comércio-e

-Instalação da ferramenta TSL

5.4.2 Etapa 2 - Configuração do sistema e ferramentas

Com o ambiente devidamente preparado e instalado, os servidores e equipamentos interligados em rede, é hora de configurar o sistemas e as ferramentas para atingir o funcionamento desejado. Inicialmente, configura-se o servidor HTTP onde deve ficar instalado o sistema de comércio-e, pois este utiliza o protocolo HTTP para disponibilizar sua interface com o usuário:

- Configuração do servidor HTTP para funcionamento e disponibilização do sistema de comércio-e.

- Configuração do módulo de segurança da rede:

- Configuração dos roteadores e comutadores
- Elaboração dos arquivos de regras dos filtro de pacotes e sistemas de detecção de intrusos.

- Configuração do protocolo TSL e certificação do servidor HTTP através do Openssl:

a) Caso a autoridade certificadora seja uma entidade externa

a.1) Gerando a chave privada do servidor[9]

openssl	genrsa	-des3	-out	servidor.cpr	2048
Comando	Gerar chave RSA	Criptografia apli-cada ao arquivo	Opção de saída para arquivos	Nome do arquivo	Tamanho da Chave

a.2) Gerando arquivo de requisição de assinatura do certificado

openssl	Req	-new	-key	servidor.cpr	-out	servidor.rac
Comando	Opção de gerar requisição	Nova requisiçao	Gerar a partir de uma chave prinvada	Arquivo da chave privada	Opção de saída	Arquivo de saída

a.3) Instalação do certificado digital no servidor HTTP

b) Caso a organização seja sua própria autoridade certificadora

b.1) Criando uma Autoridade Certificadora

b.2) Criando a chave privada da AC.

$openssl genrsa -des3 -out ac.cpr 2048

[9] Muitas empresas de certificação geram a chave privada do cliente automaticamente, logo após seu cadastro, o que torna obsoleto os passos a.1 e a.2 descritos acima.

b.3) Criando uma requisição de assinatura do certificado da AC

$openssl req -new -key ac.cpr -out requisicao.rac

b.4) Auto assinando o certificado da AC

$openssl req -x509 -days 365 -newkey rsa:2048 -keyout ac.cpr -out certificado.ctf

b.5) Gerando a chave privada do servidor

$openssl genrsa -des3 -out servidor.cpr 2048

b.6) Gerando arquivo de requisição de assinatura do certificado do servidor

$openssl req -new -key servidor.cpr -out servidor.rac

b.7) Assinando a requisição de assinatura do certificado

$openssl ca -in requisicao.rac -out certificado.ctf

b.8) Instalação do certificado digital no servidor http

- Documentação do sistema: As informações obtidas durante a fase de preparação e configuração do ambiente analisadas e adicionadas às informações do projeto do sistema fornecem uma documentação consistente do sistema, onde consta diversas informações sobre o funcionamento, configuração e manutenção.

5.5 Fase 4 - Testes

Com todo o sistema implementado, é necessário a realização dos testes iniciais. O processo de realização de testes concentra-se em: funcionamento do

sistema de comércio-e, seus aspectos lógicos internos e o funcionamento das ferramentas de segurança, com o objetivo de encontrar falhas e erros. Estes testes podem ser realizados num ambiente controlado, como uma rede interna por exemplo, e posteriormente através da disponibilização na Internet. Deve se basear num plano de testes, elaborado com a finalidade de explorar e encontrar erros no sistema.

5.6 Fase 5 - Disponibilização

O desenvolvimento de um sistema voltado á Internet exige procedimentos próprios para sua disponibilização. Primeiramente deve-se obter um endereço DNS[10] para facilitar a localização do servidor e acessar o sistema de comércio-e. No Brasil, é possível obter um endereço do tipo www.nome-empresa.com.br junto à Fapesp, que é a entidade responsável pelo domínio .br. Com o endereço eletrônico em mãos, é preciso divulgá-lo ao público desejado, além das especificações técnicas do navegador HTTP necessárias para acessar o sistema de comércio-e, pois somente alguns navegadores estão habilitados para trabalhar com o protocolo TSL, como o Netscape e o Internet Explorer, por exemplo.

5.7 Fase 6 - Manutenção

É fato que o sistema necessite ser atualizado, e que novas falhas e brechas de seguranças apareçam de tempos em tempos, além disto, o mau uso do sistema pode também prejudicá-lo e atingir sua segurança. A manutenção é uma fase

[10] DNS (Sistema de nome de domínio): Protocolo utilizado na Internet que converte nomes de domínios (ex.: www.sersoft.cjb.net) em seu respectivo número IP. As máquinas na Internet só são localizadas através de seu número IP, mas o DNS permite aos usuários fazerem uso de nomes de domínio para localizá-las, o que é mais prático.

permanente, onde a sua saída é sua própria entrada, permanecendo num ciclo constante, até o final do uso do sistema, deve basear-se nas diretivas da política de segurança da empresa e possuir um responsável pelo seu gerenciamento.

A manutenção não segue ordem definida de procedimentos, mas exige atenção e realização de atividades constantes por parte do responsável, manifestando nas seguintes formas [Maf92]:

Manutenção Corretiva: Existe quando ocorrem erros no funcionamento do sistema de comércio-e, falhas nos sistemas de segurança, como filtros de pacotes e sistemas operacionais dos servidores, permitindo o acesso indevido aos recursos do sistema ou tornado-os indisponíveis, exigindo a paralisação do funcionamento do sistema na rede e uma publicação de uma página de aviso aos usuários sobre a manutenção.

Quando os erros ocorrem com o sistema de comércio-e, estes podem ser de natureza simples, e resolvidos com algumas alterações no código. Mas quando não é possível definir a causa do problema facilmente, será preciso analisar os aspectos lógicos internos do sistema, verificado no fluxo do programa qual parte e com qual entrada ocorre o erro. É preciso ter conhecimento do funcionamento do processo e da linguagem utilizada na implementação do sistema. Após detectado e diagnosticado o erro, este pode ser corrigido e o sistema disponibilizado novamente.

Manutenção Adaptativa: Após a implantação do sistema de comércio-e, os recursos de tecnologia da informação da empresa podem sofrer adaptações, como troca dos sistema operacional por outro, além de mudanças de natureza administrativa, como mudança de pagamento via boleto bancário para cartão de crédito. A manutenção adaptativa é um processo delicado e exige o

conhecimento das diversas áreas envolvidas no procedimento, para evitar possíveis erros de funcionamento e falhas de segurança posteriormente.

Manutenção de Melhoria: O uso do sistema de comércio-e pelos clientes e seu gerenciamento pelos funcionários podem resultar em sugestões ou necessidades de melhorias, além de novos recursos que podem ser acrescentados. Esta modalidade de manutenção ocorre mais no começo da disponibilização do sistema, quando ocorrem as primeiras interações entre o sistema e seus usuários, onde podem surgir diversas sugestões e necessidades de melhorias.

Manutenção Preventiva: Esta modalidade se baseia em revisões periódicas do comportamento do sistema, corrigindo falhas encontradas e minimizando por antecipação, a ocorrência de falhas possíveis.

Capítulo 6

O Protótipo

6.1 Apresentação

Neste capítulo serão descritos os procedimentos envolvidos no desenvolvimento do protótipo baseado na metodologia apresentada neste trabalho. As informações sobre este processo servem como referência para a metodologia proposta a seguir. O protótipo é baseado numa livraria virtual, onde é possível comprar livros e outros produtos, efetuando pagamento via cartão de crédito.

6.2 Descrição do sistema

O sistema é composto de 4 módulos: institucional, divulgação, cadastro e pagamento.

O módulo institucional é um conjunto de páginas HTML que exibem informações sobre a empresa de forma interativa.

O módulo de divulgação é um conjunto de páginas HTML que exibem informações sobre os livros e outros produtos, onde é possível navegar por diversas seções, e caso esteja cadastrado, pode escolher os produtos que são armazenados temporariamente no servidor para uma possível compra, um recurso denominado "carrinho de compras".

O módulo de cadastro é responsável pelo cadastro do usuário para que ele possa utilizar o carrinho de compras e conseqüentemente efetuar transações. O cadastro possui informações importantes como nome completo, endereço, telefone, CPF e correio eletrônico. Primeiramente o usuário preenche um

formulário e envia estas informações, depois receberá uma mensagem automática no seu correio-e para que confirme seu cadastro.

O módulo de pagamento é acessado quando o usuário termina sua lista de compras e deseja efetuar o pagamento. Para acessar esta área, é preciso que o navegador reconheça o certificado digital do servidor e sua autoridade certificadora, permitindo a execução do protocolo TSL e a segurança nas transações dentro deste módulo.

6.3 Recursos disponíveis

O protótipo foi desenvolvido numa instituição já dotada de política de segurança da informação, módulo de segurança, constituído de roteador, comutador e filtro de pacotes.

6.4 Construção do protótipo

-Levantamento de informação técnica

Consulta em livros, artigos e paginas na Internet para obtenção de conteúdo sobre: Administração de Redes em Linux, Servidor HTTP Apache, Linguagem HTML, ferramentas de segurança de rede e OpenSSL.

-Escolha das Ferramentas

Diversos critérios de qualidade foram utilizados para escolha das ferramentas, entre eles podemos destacar:

- Funcionalidade: A funcionalidade do sistema deve atender às necessidades desejadas

- Segurança: O sistema deve ser robusto quanto ao controle de acesso de pessoas estranhas e não autorizadas, manter arquivos de registro dos

procedimentos.

- Eficiência: Não deve desperdiçar recursos do sistema, otimizando ao máximo o uso dos recursos necessários.

- Confiabilidade: Deve ser possível trabalhar no sistema sem o receio que este realize as tarefas solicitadas de maneira errada.

- Manutenibilidade: Os desenvolvedores devem desenvolver sistemas cujo os mantenedores possam dar o devido suporte aplicando poucos esforços.

Sendo assim, a Tabela 5.1 mostra as ferramentas escolhidas e suas principais características.

Ferramentas	**Utilizada no Protótipo**	**Características**
Sistema operacional para os servidores de rede	Linux Kernel 2.1	-Sistema operacional estável e seguro. -Sistema de arquivos e dispositivos próprio para redes. -Possui suporte e boa documentação -Código aberto (confiabilidade) -Gratuito
Servidor http	Apache	-Servidor HTTP estável e seguro -Possui suporte e boa documentação -Código aberto (confiabilidade) -Gratuito
Implementação TSL	OpenSSL	-Implementação estável e segura -Possui suporte e boa documentação -Código aberto (confiabilidade) -Gratuito

Tabela 6.1: Ferramentas utilizadas

Implementação da livraria virtual

Criação e desenvolvimento do protótipo da livraria virtual baseado na descrição do sistema. Este procedimento não será apresentado aqui, por não ser

objetivo deste trabalho, para o leitor, basta supor que um sistema como descrito na seção acima foi implementado.

Instalação e Configuração da Ferramenta OpenSSL

A instalação da ferramenta pode ser feita através da compilação de seu código fonte, o que permite ao administrador do sistema fazer adaptações, ou através do pacote compilado. Ambos estão disponíveis no sítio: http://www.openssl.org.

Inicialmente, é preciso configurar algumas diretivas em seu arquivo de configuração, baseado no modelo de autenticação e certificação escolhido. No caso deste protótipo, o modelo se baseia na criação de uma autoridade certificadora local para assinar o certificado do servidor HTTP que hospedará a livraria virtual. A seguir, serão descritos os principais comandos utilizados na linha de comando com a ferramenta Openssl:

- Criando uma Autoridade Certificadora

1-Criando a chave privada da AC

$openssl genrsa -des3 -out ac.cpr 2048

2-Criando uma requisição de assinatura do certificado da AC

$openssl req -new -key ac.cpr -out requisicao.rac

3-Auto assinando o certificado da AC

$openssl req -x509 -days 365 -newkey rsa:2048 -keyout ac.cpr -out certificado.ctf

-Gerando arquivo de requisição de assinatura do certificado

$openssl req -new -key servidor.cpr -out servidor.rac

-Assinando a requisição de assinatura do certificado

$openssl ca -in requisicao.rac -out certificado.ctf

Instalação e configuração final

Após a configuração da ferramenta OpenSSL , é preciso configurar o servidor HTTP para funcionar como autoridade certificadora e instalar seu certificado digital. Esta interface com o servidor HTTP, neste caso o Apache, é feita através da ferramenta ModSSL, disponível no sítio http://www.modssl.org.

O sistema da loja virtual deve ser instalado num diretório próprio, que será configurado no servidor HTTP como um diretório público e acessível a partir de seu endereço DNS.

Disponibilização

Após projetada e implementada toda a estrutura do sistema de comércio-e seguro, basta iniciar o servidor HTTP para que o sistema fique ativo no seu endereço DNS. Através de um navegador HTTP para internet, o sistema fica disponível na rede local e também em toda Internet.

Capítulo 7

Conclusões

A segurança da informação é fundamental para o uso da tecnologia da informação nas organizações humanas, pois somente através dela é possível gerenciar os riscos e ameaças pertinentes aos sistemas de informações. É importante ressaltar que a segurança da informação não é garantida pelas ferramentas de segurança que a organização possui, mas pela sua postura e conscientização frente à uma política de segurança compatível com a sua realidade e suas necessidades.

O protocolo TSL se apresenta como uma importante ferramenta de segurança para sistemas de comércio-e, visto que este pode garantir o sigilo das informações nas transações e a autenticação das partes envolvidas. A metodologia proposta neste trabalho contribui para uma formalização e sistematização da implantação de segurança em sistemas de comércio-e utilizando o protocolo TSL.

7.1 Trabalhos futuros

A partir da implantação e estudo da metodologia proposta, especificar e detalhar mais os procedimentos compreendidos em suas fases.

Referências Bibliográficas

[ABNT01] Artigo "Newsletter Nº20" de Abril. ABNT, Brasil, 2001 Disponível em http://www.abnt.org.br : Consultado em Janeiro/2002

[Set01] Adriana A. Sette, Segurança da Informação: Um guia para implantação e segurança básica em sistemas. Canoas, 2001

[DA99] T. Dierks, C. Allen, The TLS Protocol Version 1.0. RFC 2246, 1999

[Dwa00] Berni Dwan, There's a Great Big LEECH ON our Global Network, Computer Fraud & Security, Issue 11, Volume 2000, Elsevier Science. Disponível em http://www.sciencedirect.com : Consultado em Janeiro/2000

[Fig01] Leonardo S Figueiredo. Segurança da Informação:Segurança da Tecnologia da Informação. UFMG, Belo Horizonte, 2001

[PF00] Sônia Pantoja, Rosângela Ferreira, Evolução da Internet no Brasil e no Mundo. Ministério da Ciência e Tecnologia. Brasília, 2000

[PNS01] PESQUISA MÓDULO. 7ª Pesquisa Nacional sobre Segurança da Informação. Disponível em: http://www.modulo.com.br : Consultado em: Julho/2001

[Pres95] PRESSMAN, Roger S. Engenharia de Software. Makron Books. Rio de Janeiro, 1995

[Maf92] Bruno Maffeo, Projeto de sistemas: Engenharia de Software e Especificação de Sistemas. Editora Campus, Rio de Janeiro, 1992

[MBL00] Pedro P. Machado, Ernandes Bezerra, José O. Lima. Segurança da Informação: Fundamentos do Modelo de Segurança da Informação . Ministério do Planejamento, Brasília/DF, 2000

[Rau95] Raul. Criptografia Contemporânea. UFRGS, Porto Alegre, 1995

[Rez01] Prof. Pedro A. de Rezende, O Silêncio que Produz Ruídos. Brasília, Disponível em http://www.cic.unb.br/docentes/pedro/: Consultado em Março/2002

[TEM00] Artigos diversos - Revista Tema, ano XXVI num.175. Serpro, Brasília, 2000. Disponível em http://www.serpro.gov.br/: Consultado em Março/2002

[Suc99] Meghan Suchocki. History of E-Commerce,1999 Disponível em http://it.backmr.com.nl: Consultado em Dezembro/2001

[Tan97] Andrew S. Tanenbaum. Redes de Computadores: Redes de Computadores: Editora Campus, Rio de Janeiro, 1997

Apêndice A

Desafios para a segurança da informação

Um assunto que tem preocupado muitos especialistas da área são os sistemas de espionagem internacionais utilizados por governos de alguns países, que utilizam de sua influencia econômica e sua estrutura de telecomunicações como satélites, receptores centrais telefônicas para criarem sistemas de informação capazes de interceptar mensagens em toda rede mundial de telecomunicação, inclusive telefone, celular, correio-e e fax. Alguns destes sistemas vieram a publico, como o Echelon e o Carnivore [Dwa00].

Quando surgiram os primeiros sistemas de espionagem internacional, nos primórdios da guerra fria, a justificativa utilizada foi que era preciso espionar os inimigos com o intuito de prevenir desastres, como bombas nucleares e ataques surpresas. Atualmente, estes sistemas são utilizados, além dos objetivos de segurança, para espionagem comercial e segredos de estados [Dwa00], o que coloca em dúvida a ética e seriedade do governo destes países. Devido a estes acontecimentos, existe um grande receio na comunidade internacional em utilizar sistemas e métodos de criptografia "fechados" desenvolvidos nestes países.