Security Site – Desenvolvendo um Ambiente Seguro para E-Commerce e E-Business

Thiago de Moraes Pereira, Prof. MSc Alessandro de Castro Borges

Departamento de Computação – Universidade do Estado de Minas Gerais (UEMG)
Caixa Postal 03 – 37.900-106 – Passos – MG – Brazil

{thiagomp,acborges}@passosuemg.br

Abstract. *This paper describes a propose for a security policy in order to provide confidenciality in e-commerce and e-business transactions, with high security patterns for total control on transfered informations. The pretented solution is suited for electronic commerce, but it works too for enterpriser data transference on the Internet, or either on a Intranet and Extranet either. The presented project is on test and was developed with VPN, SSL, S-MIME, FIREWALL and ANTI-VIRUS technology.*

Resumo. *Este artigo descreve uma proposta para o desenvolvimento de uma política de segurança com o objetivo de prover confidencialidade em transações de ecommerce e e-business, atendendo aos mais altos padrões de segurança visando o controle total das informações. A solução a ser abordada não se aplica apenas ao ecommerce, mas também às empresas que necessitam fazer transferência de dados pela Internet ou até mesmo por uma Intranet e Extranet. O projeto apresentado está em fase de testes e foi desenvolvido com as tecnologias VPN, SSL, S-MIME,FIREWALL, ANTI-VÍRUS.*

1 Introdução

Com o crescimento da Internet as empresas, de modo geral, perceberam que poderiam usufruir desse ambiente para comercializar seus produtos globalmente e assim expandir seus negócios de forma abrangente, transferindo parte, ou quase a totalidade, de suas tarefas para a Internet.

Este artigo descreve o projeto Security Site, destinado a tornar seguras transações envolvendo valores, permitindo relacionamentos sem danos entre corporações e seus clientes.

1.1 Motivação

A área de segurança relacionada ao e-commerce ainda é muito incipiente no Brasil. Neste trabalho o foco não é dado apenas à venda dos produtos, mas a todos os aspectos correlacionados envolvendo clientes, comerciantes, bancos e serviços prestados. Foi desenvolvida uma proposta para solucionar deficiências de segurança no e-commerce, aumentando o grau de confiança entre clientes, comerciantes e bancos quando efetuam compras, vendas, pagamentos ou entregas pela Internet.

A solução abordada não se aplica apenas ao e-commerce, mas também às empresas que necessitam fazer transferência de dados via Internet, Intranet e Extranet.

1.2 Objetivos

O objetivo deste projeto é desenvolver uma política de segurança sólida com aplicação no e-commerce, incluindo procedimentos usados para implementar segurança em transações on-line. Outro aspecto importante é o levantamento de aspectos referentes ao tema e as variadas políticas desenvolvidas para prover segurança nas corporações.

Este trabalho solucionou divergências com relação à segurança no e-commerce e e-business. Apresentamos uma proposta de segurança às empresas que necessitam fazer transferência pela Internet com tranqüilidade e credibilidade no envio dos seus dados.

2 Projeto Security Site

O Security Site foi proposto como um trabalho para prover segurança a outro projeto de iniciação científica desenvolvido na instituição, com objetivo principal de focar todos os pontos necessários na construção de um ecommerce rentável, seguro e acessível às empresas de nossa região (a maioria de pequeno porte), aderindo à idéia de atingir um público maior, disponibilizando suas mercadorias na Internet.

O sucesso de uma organização depende em muito da maneira que trata suas informações com relação à segurança e da forma que disponibiliza seus dados. Pensando nisso, propomos uma política de segurança eficiente, eficaz e barata. Foi feita uma pesquisa minuciosa sobre os procedimentos utilizados em sites comerciais. A idéia é garantir a segurança das informações usando tecnologias vigentes no mercado.

2.1 Tecnologias Utilizadas

Foram pesquisadas várias formas de tornar um site de e-commerce seguro, levando em conta também testes em diferentes tecnologias. Abaixo estão relacionadas as que apresentaram melhores índices de credibilidade:

- **SSL** (Secure Sockets Layer) - interessante devido à sua funcionalidade em criar conexões “criptografadas” entre o servidor web e o browser, provendo segurança entre o TCP/IP e os protocolos de aplicação [Terada 2000]; [Gomes 1995].
- **VPN** (Virtual Private Network) - conexões seguras baseadas em tecnologias de criptografia, autenticação e tunelamento, [Scott 1999].
- **S-MIME** (Secure Multimedia Internet Mail Extensions) - Para um e-commerce bem sucedido, é essencial o uso do correio eletrônico no envio de mensagens entre empresas e clientes. Com base nessa idéia, a pesquisa apontou o S-MIME como uma ótima ferramenta para segurança de e-mail, pois explora uma sintaxe de mensagem “criptografada” num ambiente de Internet MIME [Smith 1997].
- **FIREWALLS -** garante integridade das informações. Impõe uma barreira entre a rede privada da organização e a rede externa, baseado na combinação de hardware e software ou somente em software [Cooper 2001], [Siyan 1995].

3 Descrição do Projeto

A proposta desenvolvida possui como um de seus critérios o poder aquisitivo de cada empresa, restringindo o nível das tecnologias e formas de proteção disponíveis de acordo com seus valores.

Em linhas gerais, o projeto coordena desde o envio das informações pelo cliente até a segurança dos dados armazenados em um determinado servidor.

3.1 Arquitetura

Com base no levantamento realizado, foi implementado um firewall para a proteção dos servidores do projeto, barrando a entrada de pacotes não identificados na rede. Na máquina firewall foram implementadas restrições acentuadas com relação à entrada dos pacotes, pois nessa máquina somente podem trafegar pacotes relacionados à porta 80, restringindo conexões de SSH, TELNET, FTP, SMTP, RIP, entre outras.

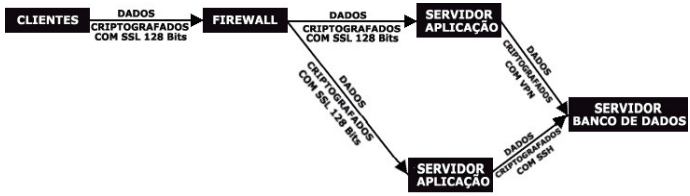

Figura 1. Diagrama de Fluxo de Dados – Trafego da informação criptografada

Foram implementadas também no firewall, restrições quanto a defensivas contra "ping da morte", "spoofing", entre outras que poderiam colocar em risco o bom funcionamento do projeto como um todo. Nessa máquina também foi implementado um sistema de balanceamento de carga entre os dois servidores de aplicação utilizados, ou seja, quando um servidor está com uma grande quantidade de serviço, requisições são redirecionadas para o segundo servidor de aplicação. Outra vantagem desse sistema se dá no caso de "negação de serviço" por um dos servidores de aplicação, quando então o outro começa imediatamente a responder todas as requisições (Tabela 1, Figura 2).

Para avaliar a aplicabilidade do balanceamento de carga, foram efetuadas grandes quantidades de requisições aos servidores de aplicação, onde os mesmos responderam de forma balanceada e dividida. Outra avaliação feita com relação ao balanceamento de carga foi a negação de serviço, onde em funcionamento um dos servidores foi reiniciado. Imediatamente o outro servidor de aplicação começou a responder as requisições que estavam sendo processadas pelo servidor reiniciado (Tabela 1).

Em resumo, quando os dois servidores estão funcionando em paralelo, a aplicação de e-commerce pode atender a uma quantidade de conexões elevada, pois se um servidor web disponibiliza uma quantidade de conexões por servidor, o balanceamento de carga irá dobrar o número de conexões, trazendo então uma maior rapidez e eficiência na disponibilização dos produtos de uma determinada empresa.

O projeto foi implementado e testado em uma rede broadcast mantendo a preocupação com relação à utilização de sniffers, pois qualquer computador em modo promíscuo poderia capturar pacotes sendo transferidos pelos servidores. Para sanar esse problema, a política de segurança descreveu a utilização de VPN e SSH entre os servidores envolvidos. Nesse caso, mesmo que o sniffer capturasse todos os pacotes,

estes estariam criptografados, conservando a transferência entre os servidores de aplicação e o servidor de banco de dados assegurada (Figura 1.).

Outra tecnologia utilizada para interligar um dos servidores foi a VPN, por ser estável e segura com relação à criptografia. As chaves geradas para "criptografar" os dados é muito grande, dificultando a quebra de sigilo do algoritmo utilizado.

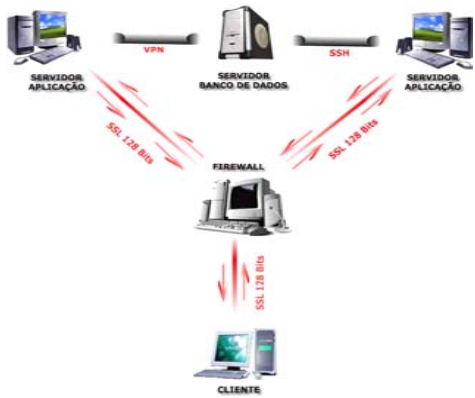

Figura 2. Solução proposta para um e-commerce e e-business seguro

O SSH foi utilizado por prover conexão "tunelada" e segura entre duas máquinas. A idéia foi criptografar os dados transferidos entre um dos servidores de aplicação e o servidor de banco de dados. Os servidores de aplicação disponibilizam uma loja de e-commerce desenvolvida em JSP, onde o cliente pode cadastrar seus dados e comprar mercadorias disponíveis. Os dados submetidos pelo cliente são enviados para o servidor de banco de dados por uma conexão "tunelada" provida pela VPN, que dá todo respaldo necessário com relação à criptografia e segurança dos dados (Figura 3).

Tabela 1. Exemplo de balanceamento de carga entre os servidores de aplicação

Requisição	Número de Requisições	% de Atendimento do Servidor de Aplicação I	% de Atendimento do Servidor de Aplicação II
Inserção	25	13	12
Consulta	25	12	13
Alteração	20	10	10
Exclusão	30	15	15
Total	**100**	**50**	**50**

Para maior segurança da proposta especificada, foi utilizado em conjunto com todas as tecnologias descritas acima o SSL de 128 bits, com o papel de criptografar os dados desde o browser do cliente até o servidor de aplicação. Para reforçar ainda mais a segurança dos servidores, foi usado IP falso. Assim, mesmo sabendo o número IP dos servidores de aplicação e também o de banco de dados, o atacante não conseguiria invadir as máquinas, pois somente o firewall responde às requisições. Quando o administrador necessita buscar algo na Internet, ou até mesmo na rede interna, por

intermédio de um servidor de aplicação, o pedido é feito, mas quem responde pelo servidor de aplicação é o firewall, e o seu é o único número IP que pode ser rastreado.

Com os mecanismos levantados uma determinada empresa pode implementar uma política de segurança levando em conta todos os aspectos citados neste artigo, atingindo altos padrões de segurança de informação com baixo custo.

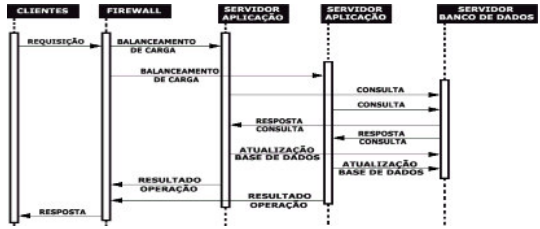

Figura 3. Diagrama de seqüência – Interação completa do usuário com a loja virtual

3.2 Resultados

Nesta seção, são apresentados os resultados obtidos a partir da simulação do modelo proposto quando submetido a várias requisições simultâneas, ataques à estrutura implementada, balanceamento de carga e negação de serviço. O estudo feito se concentra sobre a aplicação de métodos que possam assegurar transações no momento em que o cliente envia informações sigilosas para o servidor.

Na simulação, foram feitas várias requisições aos servidores de aplicação que, em conjunto com o sistema de balanceamento de carga, responderam de forma dividida e simplificada como na Tabela 1.

Após as requisições foram instalados “trojans” nos servidores, abrindo portas para invasão. Entretanto não houve efeito devido ao fato do sistema de IP falso ser capaz de proteger o restante da infra-estrutura. A título de simulação, um sniffer foi instalado em uma máquina à parte e conectada à rede dos servidores (interna ao firewall) para que pudesse capturar dados transferidos entre eles. Foram feitas novas requisições após a existência do sniffer, e todos os pacotes transferidos do cliente para os servidores foram “criptografados” conforme a análise do relatório gerado pelo sniffer.

Outra simulação tentou estabelecer conexões SSH, barradas pelas restrições aplicadas ao firewall. Conexões TELNET e FTP, bem como o “ping da morte", também foram barradas, trazendo maior confiabilidade ao restante dos servidores.

4 Conclusão

Nosso trabalho focou, de forma ampla e abrangente, tecnologias disponíveis no mercado que provêem segurança em sites de e-commerce e e-business, despontando como mais utilizadas (VPN, SSL, FIREWALL, ANTI-VÍRUS), citando também a política de segurança para os meios físicos onde a aplicação será implementada.

Este trabalho descreve uma proposta para acesso a uma loja de e-commerce, permitindo diversos níveis de segurança para com os clientes e para com a infraestrutura envolvida, validada através de simulações como compras na loja implementada, e

também tentativas de ataques ao firewall e aos servidores de aplicação. Com base nos valores para aquisição das tecnologias avaliadas foi desenvolvida uma política de segurança acessível às empresas da região da pesquisa.

Acreditamos que o resultado deste trabalho tem muito a contribuir com as empresas da região, oferecendo-lhes condições de ganho de mercado (usando a Internet) de forma segura e com custo aceitável.

5 Trabalhos Futuros

O próximo passo em busca de integridade nas transações entre cliente/servidor é agregar a idéia de Sistemas Distribuídos ao projeto, efetuando, por intermédio de uma rede, rastreamento em máquinas clientes. O trabalho terá como funcionalidade:

- Manter no servidor uma lista com a cópia de todos os arquivos que compõem uma determinada máquina na rede.
- Efetuar uma varredura completa em busca de todos os arquivos instalados e gerar um valor para controle sempre que a máquina cliente for iniciada.
- Se o valor recém-processado diferir daquele no servidor, verificar o motivo da diferença comparando a lista do servidor com uma lista de arquivos do cliente.
- Se constatados arquivos no cliente além dos presentes na lista do servidor, apagar os excedentes, tendo em vista que os arquivos necessários para o bom funcionamento da máquina sempre serão os mesmos.
- Se constatada, entretanto, a falta de arquivos na máquina cliente, verificar na lista quais arquivos, e imediatamente iniciar as cópias necessárias.
- No caso de listas iguais, iniciar varredura em busca de vírus e vulnerabilidades que permitam interceptação de dados ainda não “criptografados”.
- Se encontrada alguma vulnerabilidade, vírus ou trojan, gerar um arquivo de notificação (log) para o administrador da rede. A máquina fica restrita ao uso até o administrador desbloquear o sistema efetuando as devidas correções.
- Feitas as correções requerer o reinício da máquina, provocando nova verificação.

6 Referências Bibliográficas

Cooper, S. Construindo um firewall para Internet. Rio de Janeiro: Campus, 2001.

Gomes O. Segurança Total: protegendo-se contra hackers. São Paulo: Makron Books, 1995.

Scott, C. Virtual Private Networks. Beijing: O’illy, 1999.

Siyan, Katarine Internet Firewalls and Network Security. Indianapolis: New Riders Publishing, 1995.

Smith, R. E. Internet Criptography. Addison Wesley Longman, Massachussets: 1997.

Terada, R. Segurança de Dados: criptografia em redes. São Paulo: Edgard Blucher, 2000.

Scambray, J. Hackers Expostos: 2ª Edição. Makron Books, 2001.