PROTOCOLO HTTP X PROTOCOLO HTTPS

SILVA, André Luis de Souza[1]

SILVA, Regina Célia Marques Freitas [2]

Recebido em: 2008-10-13

Aprovado em: 2009-04-06

ISSUE DOI: 10.3738/1982.2278.146

RESUMO: A Internet passou a ter notoriedade nas empresas como um diferencial competitivo, podendo expandir seus negócios mundialmente. Este mercado gigantesco que está em constante evolução proporciona imensas expectativas de bons negócios. Por outro lado, existe uma grande ameaça as empresa e aos usuários da Internet. Com o risco eminente de uma informação sigilosa ser interceptada, faz com que, os usuários se tornem inseguros ao disponibilizar informações via Web. Este trabalho se propõe a discutir a forma de transmissão de dados pela Internet, fazendo uma comparação entre transmissão de dados via protocolo http e https.:

Palavras-chave: Internet. Protocolo HTTPS. Protocolo HTTP, criptografia.

SUMMARY: The Internet had a reputation in the business as a competitive differential and may expand its business worldwide. This huge market that is constantly evolving provides enormous expectations of good business. On the other hand, there is a great threat to the company and users of the Internet. With the imminent risk of confidential information being intercepted, causes, users become unsafe to provide information via Web This paper aims to discuss the form of data transmission over the Internet, making a comparison of data transmission via http and https protocol.

Keywords: Internet. HTTPS protocol. HTTP protocol, cryptography.

INTRODUÇÃO

"A infra-estrutura inicial da Internet não permitia as transações *on-line*[...]" (STALLEINGS, 2005, p. 68) A falta de uma interface amigável com o usuário, da segurança na transmissão, e das formas de pagamentos seguras, sempre estiveram em pauta quando se tratava da continuidade do avanço da Internet.

[1] Graduando em Sistemas de Informação

[2] Coordenadora do curso de Sistemas de Informação FE/FAFRAM

A Internet hoje, se tornou mais que um agente de comunicação e informação, podendo dizer que a mesma foi um motor da revolução, que está modificando as formas tradicionais de fazer negócio.

"Os navegadores de hoje admitem a comunicação segura com o servidor para o preenchimento de formulário e o fornecimento de informações de cartão de credito." (STALLEINGS, 2005, p. 68)

Com o aumento da base de dados de usuário e a Internet sendo uma via aberta, torna-se necessário obter conhecimentos de como funciona a transmissão de dados para não correr o risco de que um pacote de informação seja interceptado e lido por qualquer pessoa da via.

Sendo a Internet um veículo ágil e eficaz no intercâmbio de correspondências, surgiu a necessidade de que apenas o remetente e o receptor pudessem ter acesso aos dados dos documentos envolvidos na transação, através de um meio técnico que fosse capaz de garantir a inviolabilidade.

A segurança na transmissão, mais especificamente a criptografia de dados que, "são necessárias para proteger os dados durante sua transmissão e para garantia que as transmissões de dados sejam autenticas". (STALLEINGS, 2005, p. 380).

Como descreve Tanenbaum, (2003, p. 768) "a autenticação cuida do processo de determinar com quem você está se comunicando antes de revelar informações sigilosas ou entrar em uma transação comercial."

Observa-se o ponto relevante: que a credibilidade de uma informação esta ligadas a sua originalidade e a certeza de que a informação não foi corrompida pelo caminho que percorreu até chegar ao destinatário.

O presente trabalho traça uma panorâmica acerca da Internet, com seus desdobramentos técnicos e práticos para garantir que uma transmissão seja considerada segura, demonstrando através de um aplicativo que envia e recebe dados criptografados e não criptografados de um servidor.

PROTOCOLO HTTP

1. "*Hypertext Transfer Protocol* (HTTP[3]) é o protocolo básico da *World Wide Web* (WWW) e pode ser usado em qualquer aplicação cliente/servidor que envolve hipertexto."(STALLINGS, 2005, p. 121)

[3] HTTPS *Hypertext Transfer Protocol* (protocolo da camada de implementação)

2. O HTTP foi desenvolvido para ser usado na Internet, embora seu desenho definitivo permita que ele possa ser usado em outras formas de aplicação. “Por essa razão, são aceitas operações chamadas método diferente da simples solicitação de uma página da web.” (TANENBAUM, 2003, p. 694) Essas solicitações são feitas através de linhas de textos ASCII[4], (*American Standard Code for Information Interchange*) onde, a primeira palavra da primeira linha é o nome do método.

3. A confiabilidade das informações em uma transmição HTTP e feita com o protocolo TCP (*Transmission Control Protocol*), apesar disso, HTTP é um protocolo sem estado, ou seja, cada comunicação e tratada independentemente.

PROTOCOLO HTTPS

HTTPS[5] (*Hypertext Transfer Protocol Secure*) é a variação do protocolo HTTP com o protocolo SSL[6] (Secure Sockets Layer) que é um protocolo proposto pela Netscape em 1994 com apoio da Verisign e da Sun, e foi lançado inicialmente em 1994.

HTTPS é um protocolo que tem por finalidade garantir a segurança na transmissão de dados, em aplicações que envolvam dados sigilosos, como o e-commerce, transação bancária, senhas, informações privadas e tantas outras.

Para o *browser* o protocolo HTTPS e considerado único, mesmo sendo a junção de dois protocolos, sendo assim, é necessário utilizar https: // sempre que for chamar uma página com segurança, e http:// para as páginas sem segurança.

Todas as transferências entre browser e servidor com protocolo HTTPS serão criptografados, e simbolizados por um cadeado na barra de status que deve estar fechado para caracterizar a devida segurança, esse protocolo usa a porta lógica 443 definida pela IANA[7] (Internet Assigned Numbers Authority).

CONDIÇÃO PARA O USO DO PROTOCOLO HTTPS

O HTTPS como foi visto é um protocolo HTTP com SSL, tornando assim um protocolo com segurança. Para que as transmissões com segurança ocorram o HTTPS deve estar ativado no servidor, e o browser do cliente deve estar habilitado com o

[4] ASCII *American Standard Code for Information Interchange* (Código Padrão Americano para o Intercâmbio de Informação)
[5] HTTPS (*Hypertext Transfer Protocol Secure)* protocolo HTTP com Segurança
[6] SSL *(Secure Sockets Layer)* protocolos criptográficos
[7] IANA[7] (*Internet Assigned Numbers Authority*).

protocolo SSL. Hoje no mercado a maioria dos browsers já é habilitada para o protocolo SSL.

Embora muitos sites com segurança utilizem o protocolo HTTPS na maioria dos casos não é necessário digitar um URL[8] (*Uniform Resource Locator*) utilizando HTTPS, pois normalmente ela estará em uma página HTTP, que só iniciará a conexão segura quando por algum link direcionará a página atual para uma página com segurança. No momento que a URL apresentar "https: //" um ícone de cadeado aparecerá na barra de status ou na barra superior browser dependendo da sua versão, podendo assim tomar informações sobre a certificação digital.

O uso da certificação digital e fundamental para a ativação do HTTPS, logo, como todo servidor deve ter HTTPS ativado, o mesmo deve ser certificado.

Por trás de tudo que um certificado digital representa esta à garantia que o cliente estará enviando dados para a host correta, isto é, o servidor é mesmo quem diz ser, pois quando abrimos um site seguro as especificações da certificação estarão todas disponíveis ao clicarmos na figura do cadeado que aparecera no browser. Figura 1.

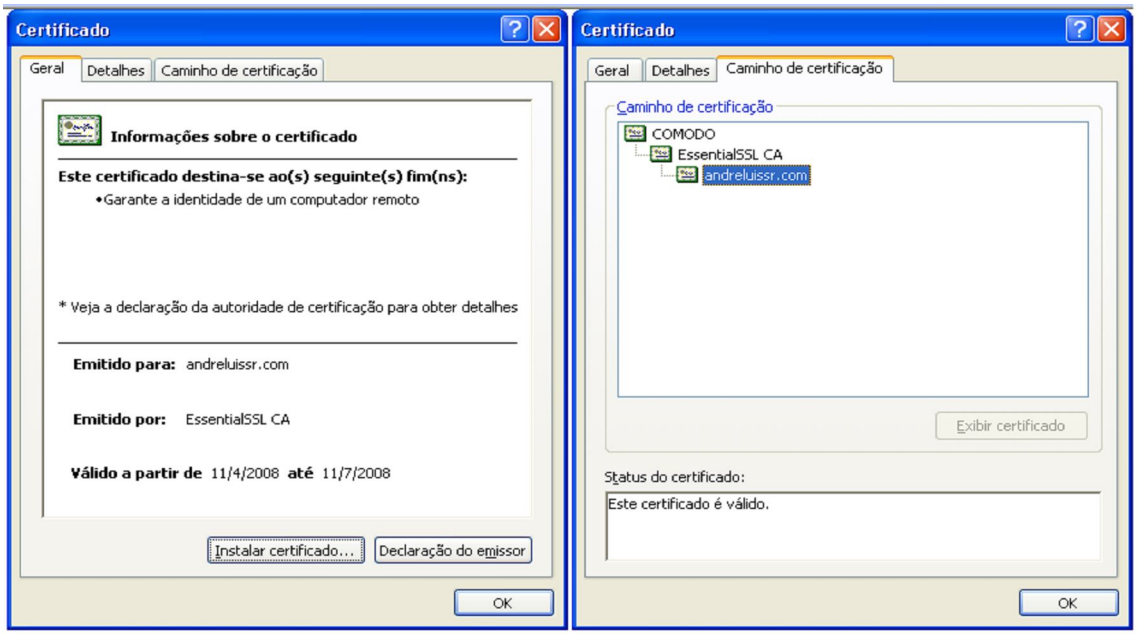


FIGURA 1: Certificação SSL

COMPARAÇÃO HTTP X HTTPS

Para a realização dessa comparação alguns requisitos foram essenciais, como:

a) Hospedagem: Foi contratado um serviço de hospedagem, com suporte PHP e protocolo SSL.

[8] URL (*Uniform Resource Locator*) Localizador Uniforme de Recursos.

b) Domínio: Foi registrado um domínio www.andreluissr.com

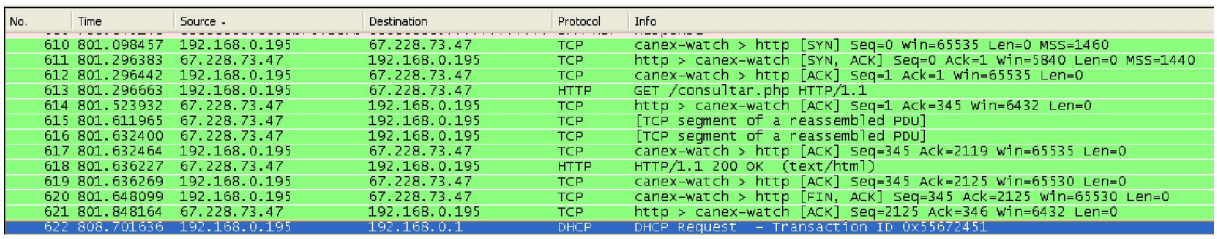
c) IP fixo: Foi contratado um IP fixo.

d) Certificação SSL: Foi contratado uma certificadora SSL, na COMODO BRASIL

e) Ethereal, um poderoso *sniffe*[9]*r*, ele pode ser usado tanto para proteger seu sistema quanto para roubar dados dos vizinhos, uma faca de dois gumes, por isso ele é às vezes visto como uma "ferramenta *hacke*[10]*r*" quando na verdade o objetivo do programa é dar a você o controle sobre o que entra e sai da sua máquina e a possibilidade de detectar rapidamente qualquer tipo de *trojan*, *spyware* (vírus) ou acesso não autorizado.

Para começar foi utilizada uma ferramenta para capturar os pacotes enviados e recebidos pelas solicitações feitas pelos protocolos HTTP e HTTPS. Essa ferramenta foi o Ethereal.

Primeiramente foram enviadas ao banco de dados, através do formulário criado, informações usando protocolo HTTP, logo em seguida foram capturados os pacotes pertinentes a essas informações, usando a função do Ethereal que inicia a filtragem da rede'*CaptureStart*'.



No.	Time	Source	Destination	Protocol	Info
610	801.098457	192.168.0.195	67.228.73.47	TCP	canex-watch > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
611	801.296383	67.228.73.47	192.168.0.195	TCP	http > canex-watch [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1440
612	801.296442	192.168.0.195	67.228.73.47	TCP	canex-watch > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
613	801.296663	192.168.0.195	67.228.73.47	HTTP	GET /consultar.php HTTP/1.1
614	801.523932	67.228.73.47	192.168.0.195	TCP	http > canex-watch [ACK] Seq=1 Ack=345 Win=6432 Len=0
615	801.611965	67.228.73.47	192.168.0.195	TCP	[TCP segment of a reassembled PDU]
616	801.632400	67.228.73.47	192.168.0.195	TCP	[TCP segment of a reassembled PDU]
617	801.632464	192.168.0.195	67.228.73.47	TCP	canex-watch > http [ACK] Seq=345 Ack=2119 Win=65535 Len=0
618	801.636227	67.228.73.47	192.168.0.195	HTTP	HTTP/1.1 200 OK (text/html)
619	801.636269	192.168.0.195	67.228.73.47	TCP	canex-watch > http [ACK] Seq=345 Ack=2125 Win=65530 Len=0
620	801.648099	192.168.0.195	67.228.73.47	TCP	canex-watch > http [FIN, ACK] Seq=345 Ack=2125 Win=65530 Len=0
621	801.848164	67.228.73.47	192.168.0.195	TCP	http > canex-watch [ACK] Seq=2125 Ack=346 Win=6432 Len=0
622	808.701636	192.168.0.195	192.168.0.1	DHCP	DHCP Request - Transaction ID 0x55672451

FIGURA 2: Pacotes capturados HTTP**.**

A princípio podemos notar que nessa transmissão foi usado o protocolo de transporte TCP, que fica abaixo da camada de aplicação, que e o HTTP, que também foi usado.

Se observar mos cada pacote individualmente usando a função "*Follow* TCP *Striam*" nota-se que as informações estão vulneráveis podendo ser receptadas por terceiro e fazendo mau uso das mesmas.

9 *Sniffe (*espião da rede), uma aplicação que fica entre a comunicação entre hosts da rede.

10 *Hacker* individuo com grande conhecimento em computadores que usa seus conhecimentos para roubar informações da rede.

FIGURA 3: Mensagens capturadas HTTP**.**

O mesmo princípio foi feito para transmitir dados usando o protocolo HHTTPS

.

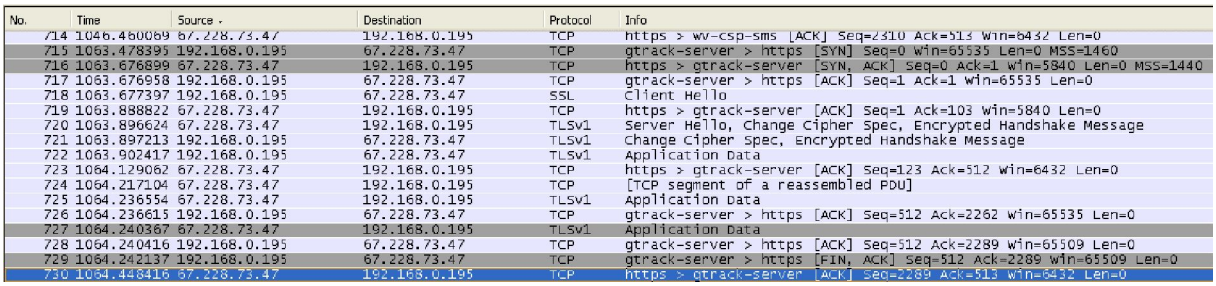


FIGURA 4: Pacotes capturados HTTPS**.**

Neste caso podemos observar que além do protocolo TCP, apareceu os protocolos SSL (*Secure Sockets Layer*) que está entre a camada de transporte e a camada de aplicação, e o protocolo TLS (*Tranport Layer Security*) que é um protocolo de transporte, que apenas pelos nomes citados percebe-se que se trata de protocolos de segurança.

Observando individualmente esses protocolos não fica duvida que realmente são protocolos que criptografam as informações da transmissão realizada, as informações contidas nessa figura e a mesma da figura 3, com a diferença de estarem cifradas.

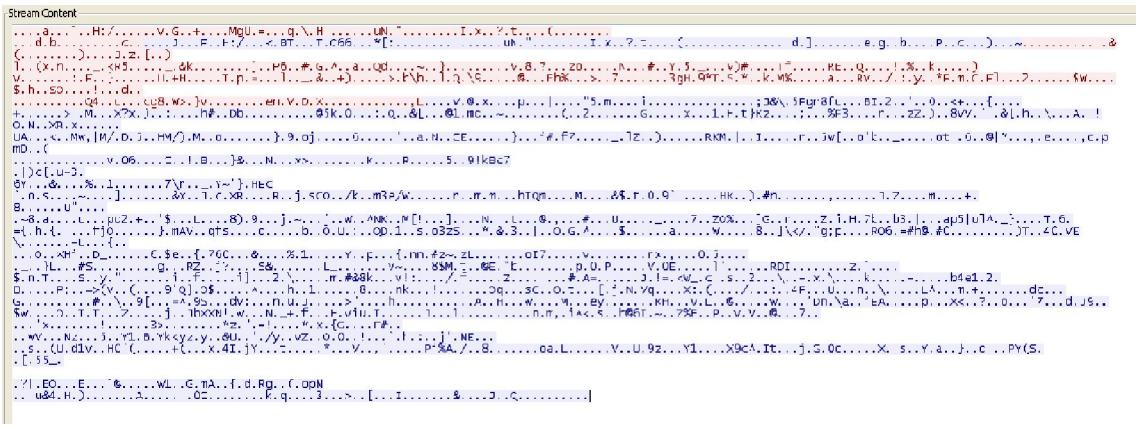


FIGURA 5: Mensagem capturada HTTPS.

CONCLUSÃO

Com o crescimento da informática em todas as áreas proporcionou que a segurança fosse colocada em destaque, e hoje não se fala em Internet sem ao menos contestar do nível de segurança que a mesma proporciona, principalmente nas áreas financeira.

A contribuição desse trabalho foi demonstrar com termos técnicos e aplicativos, como a Internet trata uma transmissão de dados sem criptografia e com criptografia.

A principal dificuldade encontrada foi gerar um certificado SSL, pelo fato que essa certificação não funciona localmente, exigindo alguns requisitos como: IP fixo, domínio e um servidor seguro.

A demonstração proporciona uma tranqüilidade ao usuário da Internet que tenha receio em efetuar transações via Web, sabendo agora identificar um site seguro e como seus dados chegarão até o servidor e que mesmo se essas mensagens forem interceptadas, não servirão de nada ao individuo se ele não possuir a chave de criptografia.

REFERENCIAS

CHAVES, S. M. Disponível em: < http://www.inf.pucrs.br/~mchaves/pg_portugues/tc/paperxml.pdf >. Acesso em 01 mai.2008, 19:30h.

D`ÂNGELO, F. **O que é ASP? .** Disponível em: < http: //www.aspbrasil.com.br/conteudo/detalhesCompleta.aspx?codConteudo=3425&Secao= TUTORIAIS > . Acesso em 12 mai.2008, 23:00.

GRAEML, A. R**. Sistemas de informação:** o alinhamento da estratégia corporativa. 2. ed. São Paulo: Atlas, 2003.

JAVA FREE. **O que é Java?**. Disponível em: < http://www.javafree.org/content/view.jf?id Content=84>. Acesso em 01 mai.2008, 14:55h.

KUROSE, J. F.; ROSS, K. R. **Redes de Computadores e a Internet:** uma nova abordagem. 1. ed. São Paulo: Addison Wesley, 2003

LAUDON, K. C. **Sistemas de informações gerenciais:** Administrando a empresa digital. São Paulo: Prentice Hall, 2004.

PICARELLI, J. E. Disponível em: <http://www.dca.fee.unicamp.br/courses/IA368F/ 1s1998/ProgWeb/b5.html.> Acesso em 12 mai.2008, 23:45h.

REZENDE, D. A.; ABREU, A. F. de. **Tecnologia da informação aplicada a sistemas de informação empresariais**. 4. ed. – São Paulo: Atlas, 2006.

STALLINGS, W. **Redes e sistemas de comunicação de dados:** teorias e aplicações corporativas. 5 ed. Rio de Janeiro: Elsevier, 2005.

TANENBAUM, A. S. **Redes de Computadores.** Rio de Janeiro: Elsevier, 2003 – 9ª reimpressão.