Segurança em Redes

Aula 14 - O Protocolo HTTPS (HTTP Secure)

Apresentação

Nesta aula, iremos estudar o protocolo HTTPS (*HyperText Transfer Protocol Secure*), uma implementação do protocolo http://pt.wikipedia.org/wiki/HTTP com uma camada adicional de segurança. Estudaremos o que é o protocolo, quando usar, quando não usar e os problemas do HTTP que foram determinantes para o surgimento do HTTPS.

Vídeo 01 - Apresentação

Objetivos

Ao final desta aula, você será capaz de:

- Conhecer a solução de segurança para o HTTP.
- Saber em quais situações usar o HTTPS.
- Saber quando não usar o HTTPS.

Conceito Geral de HTTP e HTTPS

Na disciplina de Redes de Computadores, você estudou um protocolo que já devia utilizar, ou pelo menos conhecer, mesmo antes de iniciar este curso: o HTTP (*HyperText Transfer Protocol*), que é um protocolo de comunicação amplamente usado no acesso a páginas na internet. Esse protocolo não contempla soluções de segurança. Para resolver esse problema, o HTTP foi alterado, de forma a incluir suporte à transmissão por meio de uma conexão criptografada e verificação da autenticidade do servidor e do cliente. Surgiu, então, o HTTPS (*HyperText Transfer Protocol Secure*), uma implementação do protocolo HTTP sobre uma camada SSL (*Secure Socket Layer*) ou TLS (*Transport Level Security*). Essa camada adicional permite que: (i) os dados sejam transmitidos por meio de uma **conexão criptografada**; (ii) seja possível verificar a **autenticidade** do servidor e do cliente, usando **certificados digitais**, que você já estudou no nosso curso.

Como vocês sabem, o protocolo HTTP é bastante simples, com comandos em formato de texto, transportado através de uma conexão TCP (em geral na porta 80), que tem o objetivo de enviar requisições a servidores, na forma de URL, e obter respostas na forma de conteúdos especificados pelo padrão MIME.

Para o protocolo HTTPS, a porta TCP usada é a 443. O protocolo HTTPS é usado quando se deseja evitar que a informação transmitida entre o cliente e o servidor seja visualizada por terceiros. Existem vários casos onde é necessária essa segurança, por exemplo, quando você está inserindo seu login e senha para entrar em um webmail; quando você está realizando transações financeiras como acesso a uma página de um banco, e até mesmo quando você está usando uma das redes sociais.

Como ilustrado na **Figura 1**, quando você acessa uma página, o uso do HTTPS pode ser facilmente identificado na barra de endereços e de tarefas. Veja que nas URL aparece no início "https://", e do lado direito aparece um cadeado que demonstra a certificação de página segura (SSL). Alguns navegadores indicam um site seguro através das barras de endereço que ficam verde. Consulte a ajuda do seu navegador para mais informações de como ele avisa sobre sites seguros.

Figura 01 - Indicação do uso do https

Fonte: http://c10.quickcachr.fotos.sapo.pt/i/mee05404f/7753991_EiYAP.jpeg Acesso em: 03 set. 2012

Atenção!

Nunca revele o seu número do cartão de crédito através de uma página/site iniciada por http://. Ela não é uma conexão segura, seus dados podem ser interceptados.

Atividade 01

1. Por que é importante usar HTTPS no lugar do HTTP?

Problemas de Segurança com o HTTP

Por que HTTP não oferece a mesma segurança do HTTPS?

- Porque as informações navegam na rede da mesma maneira que é a apresentada na tela ou digitadas pelo usuário, ou seja, se o login e senha do usuário, por exemplo, são inseridos no pacote de dados e enviados via rede. Esses dados podem ser interceptados e o intruso recupera o login e senha do usuário.

- Porque não garante que a página acessada é a página real. Pode ser acessada uma página falsa e o usuário pensar que está usando a página verídica. Por exemplo, no caso de um banco, o usuário poderá inserir os seus dados bancários que serão roubados pelos proprietários da página falsa.

Vídeo 02 - Problemas de Segurança

Funcionamento do HTTPS

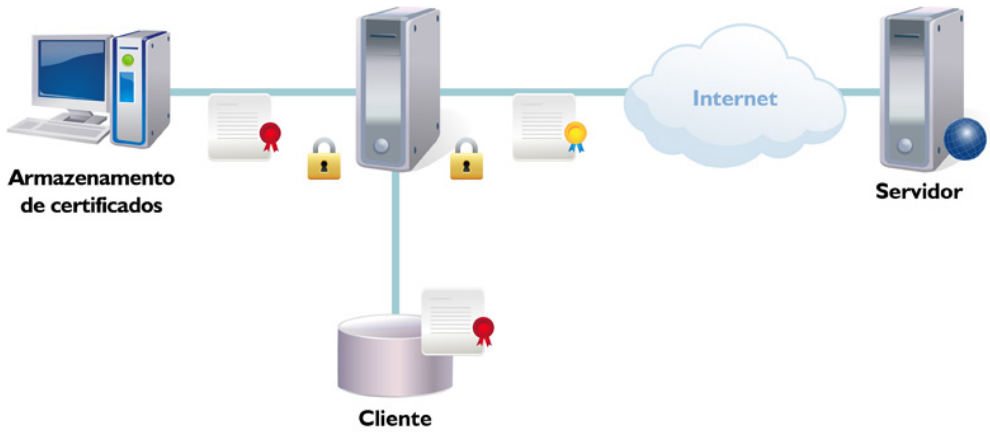
O protocolo HTTPS usa os ***certificados SSL*** para criptografar dados online. Com os dados criptografados, mesmo se alguém interceptar a mensagem, não conseguirá entende-la. Apenas o emissor e o receptor, que conhece o certificado, consegue decriptar a mensagem. Os certificados SSL contém uma chave pública do proprietário do computador e esse proprietário compartilha a chave pública com quem precisa, de forma que outros usuários podem encriptar as mensagens para o proprietário. Durante a transferência, a confiabilidade fica por conta do protocolo TLS/SSL. Na mensagem HTTPS tudo é criptografado: cabeçalhos, requisições e respostas.

O protocolo SSL é adequado para uso com o HTTP porque pode fornecer proteção, mesmo se apenas uma das partes da comunicação seja autenticada. Isso é muito comum nas transações HTTP na internet, em que, em geral, apenas o servidor é autenticado. Essa autenticação ocorre via verificação do certificado do servidor realizada pelo cliente.

Como o HTTPS é um canal seguro sobre uma rede insegura, ele protege a comunicação de escutas ilegais (*eavesdropping*) e de ataques de homem-no-meio (*man-in-the-middle*). Você lembra que estudamos esses dois problemas de segurança? Para relembrar: *Eavesdropping* é uma técnica para violação da confidencialidade que realiza leitura não autorizada de mensagens. Já homem-no-meio é a técnica de se interpor algo no meio de uma comunicação.

A **Figura 2** ilustra a comunicação entre cliente e servidor usando HTTPS. Os certificados são armazenados e a comunicação que flui entre cliente e servidor é criptografada usando a chave contida no certificado.

Figura 02 - Comunicação entre cliente e servidor usando HTTPS.



Fonte: Autoria Própria

Vídeo 03 - HTTPS

Quando não Usar HTTPS?

Não se devem usar páginas seguras quando não for necessário, pois esse protocolo requer processamento a mais do que o HTTP, para a função de encriptação. Além disso, essas páginas não ficam guardadas em cache, então, toda vez elas são requisitadas novamente.

Atividade 02

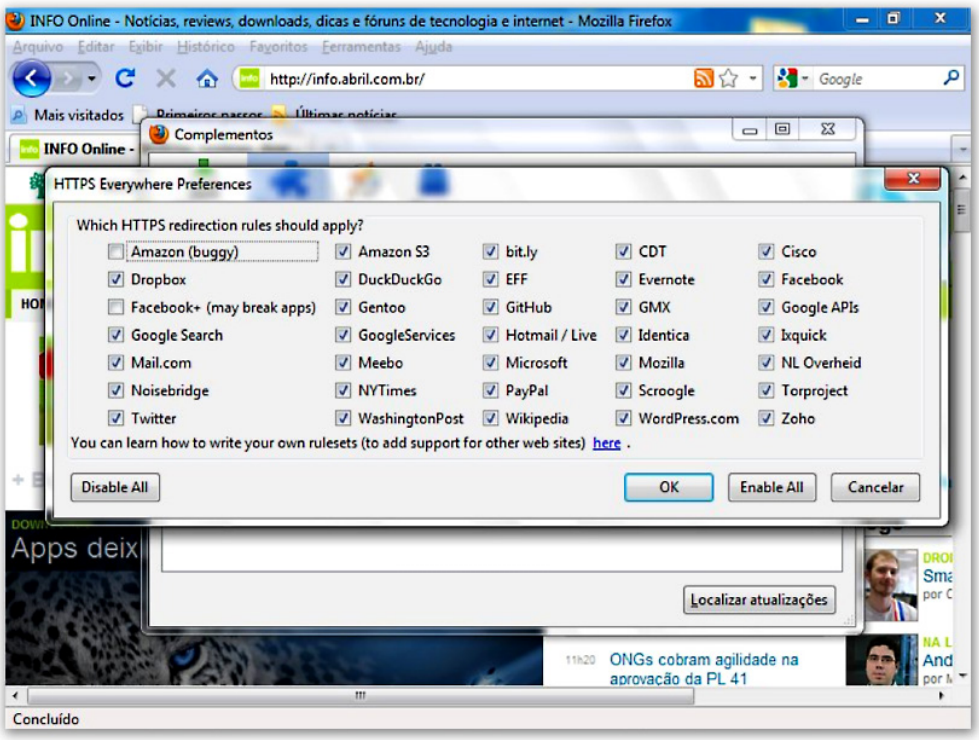
1. O que é criptografado quando usamos o HTTPS?

Garantindo HTTPS no Firefox e no Chrome

O HTTPS Everywhere é um projeto da *Fundação Frontier Foundation* (EFF) e da *The Tor Project*, cujo objetivo é identificar falhas de segurança em sites visitados a partir do navegador Mozilla Firefox. O *HTTPS Everywhere* é um complemento (*add-on*) para o Firefox, com a finalidade de deixar a navegação na web mais segura. Com esse complemento ativado, o usuário acessa diversas páginas web por meio do protocolo HTTPS. Segundo os desenvolvedores da ideia, várias páginas oferecem a possibilidade de navegação com o HTTPS, mas, com a dificuldade de uso, a navegação padrão acaba sendo no HTTP. O *HTTPS Everywhere* resolve esse problema e possibilita que o usuário navegue de forma segura. Esse complemento também pode ser usado no navegador Chrome.

A **Figura 3** ilustra a janela onde são escolhidas as preferências do usuário em relação ao uso do HTTPS. Observe que o usuário marcou que todas as páginas web devem ser acessíveis via HTTPS, exceto a Amazon (buggy) e o Facebook+.

Figura 03 - HPPTS Everywhere no Mozila.



Fonte: http://info.abril.com.br/noticias/blogs/download-da-hora/files/2011/01/HTTPS-Everywhere-1.jpg Acesso em: 03 set. 2012

Atenção!

O HTTPS não deve ser confundido com o protocolo "Secure HTTP" (S-HTTP), especificado na RFC 2660, que é menos usado que o HTTPS.

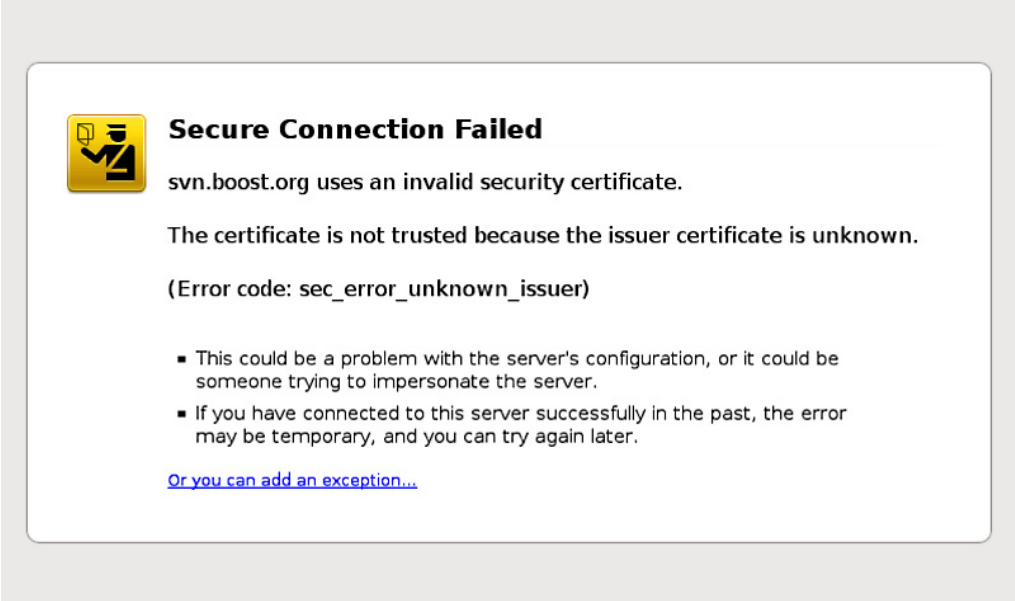
Confiança Provida pelo HTTPS

A confiabilidade da conexão HTTPS é baseada em Certificados Digitais, fornecidos por autoridades de certificação. Elas vêm pré-instaladas no navegador. Uma conexão HTTPS pode ser confiável se e somente se todos os itens a seguir são verdade [Fonte: Wikipedia]:

- O usuário confia que o navegador usa o HTTPS com autoridades de certificação pré-instaladas de forma adequada.
- O usuário confia que as autoridades verificadoras só irão confiar em páginas legítimas.
- A página acessada fornece um certificado válido, o que significa que ele foi assinado por uma autoridade de certificação confiável.
- O certificado identifica corretamente a página.
- O tráfego na internet é confiável devido à camada de encriptação do protocolo TLS/SSL.

Os navegadores mostram um aviso se recebem um certificado inválido, como ilustra a **Figura 4**, que mostra ao usuário um aviso em uma caixa de diálogo e perguntam se ele deseja continuar, adicionando uma exceção.

Figura 04 - Navegador exibindo que o certificado não é confiável.



Fonte: http://www.tip.net.au/wiki/index.php/Firefox_3_-_Secure_Connection_Failed Acesso em: 03 set. 2012

Vídeo 04 - Configuração SSL

Atividade 03

Pesquise

1. Gostou do tema? Então pesquise mais sobre como configurar o Apache usando SSL: http://www.conectiva.com.br/apache9.ssl.sgml.html. Acesso em: 01 ago. 2012.

Resumo

Nesta aula, você aprendeu mais sobre como tornar o acesso a páginas web seguro, usando HTTPS. Você também aprendeu que o HTTPS usa o SSL/TLS para permitir a criptografia dos dados trocados entre clientes e servidores. Você deve lembrar algo semelhante em relação a aulas anteriores sobre o POP, SMTP. Além disso, também aprendeu sobre o *HTTP Everywhere*, quando usar e quando não usar o HTTPS.

Autoavaliação

1. Por que a segurança é importante para as páginas web?
2. Como se identifica que o https está sendo usado em uma página web?
3. Por que SSL é adequado a HTTP?
4. Marque Verdadeiro ou Falso nas assertivas a seguir:

   ( ) Sempre deve-se usar o HTTPS, não há desvantagens no seu uso.
   ( ) HTTP e HTTPS usam a mesma porta: 80.
   ( ) No HTTPS, os dados são encriptados usando certificados SSL.
   ( ) O *HTTPS Everywhere* tem como finalidade deixar a navegação na web mais segura.

Referências

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet**. Amsterdam: PEARSON EDUCATION , 2010.

WIKIPEDIA. Disponível em: <http://pt.wikipedia.org/wiki/HTTPS>. Acesso em: 03 set. 2012.