UNIVERSIDADE ESTADUAL DA PARAÍBA – UEPB
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS – CCEA

CAMADA DE APLICAÇÃO

PROTOCOLOS - continuação

Ingrid Morgane Medeiros de Lucena

❑ **HTTPS** (Hyper Text Transfer Protocol Secure)

- É uma implementação do protocolo HTTP sobre uma camada adicional de segurança que utiliza o protocolo SSL/TLS.

- Essa camada adicional permite que os dados sejam transmitidos por meio de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente por meio de certificados digitais. A porta TCP usada por norma para o protocolo HTTPS é a 443.

❑ HTTPS

• O protocolo HTTPS é utilizado, em regra, quando se deseja evitar que a informação transmitida entre o cliente e o servidor seja visualizada por terceiros, como por exemplo no caso de compras *online*.

• A existência na barra de endereços de um cadeado (que pode ficar do lado esquerdo ou direito, dependendo do navegador utilizado) demonstra a certificação de página segura (SSL/TLS).

• A existência desse certificado indica o uso do protocolo HTTPS e que a comunicação entre o browser e o servidor se dará de forma segura. Para verificar a identidade do servidor é necessário um duplo clique no cadeado para exibição do certificado.

❑ HTTPS

- A ideia principal do HTTPS é criar um canal seguro sobre uma rede insegura.

- Isso garante uma proteção razoável de pessoas que realizam escutas ilegais (os chamados eavesdroppers) e de ataques de homem-no-meio (man-in-the-middle), dado que a cifragem foi adequadamente utilizada e que o certificado do servidor é verificável e confiável.

❑ HTTPS

Aspectos técnicos

Diferenças para o HTTP

As URLs HTTPS começam com https:// e utilizam a porta 443 como padrão ou, alternativamente, 8443, enquanto as URLs HTTP começam com http:// e utilizam a porta 80 como padrão.

HTTP é inseguro e sujeito a ataques de homem-no-meio e escutas ilegais, que podem levar a atacantes ganharem acesso a informações sensíveis.

O HTTPS foi projetado para proteger contra esses ataques e é considerado seguro contra eles (com exceção de versões mais antigas e obsoletas do SSL).

❑ HTTPS

Aspectos técnicos

HTTP opera na camada superior do Modelo OSI, a camada de aplicação, **mas o protocolo de segurança opera em uma subcamada inferior, criptografando uma mensagem HTTP antes de sua transmissão e decriptando a mensagem assim que ela chega ao destino.**

HTTPS não é um protocolo separado, mas se refere ao uso do HTTP sobre uma camada encriptada de conexão SSL/TLS.

Tudo na mensagem HTTPS é criptografado, incluindo os **cabeçalhos, as requisições e respostas.**

❑ TLS

O **Transport Layer Security** (**TLS**), assim como o seu antecessor *Secure Sockets Layer* (**SSL**),é um protocolo de segurança projetado para fornecer segurança nas comunicações sobre uma rede de computadores.

Várias versões do protocolo encontram amplo uso em aplicativos como navegação na web, email, mensagen instantâneas e voz sobre IP (VoIP).

Os sites podem usar o TLS para proteger todas as comunicações entre seus servidores e navegadores web.

O protocolo TLS visa principalmente fornecer privacidade e integridade de dados entre dois ou mais aplicativos de computador que se

❑ TLS

- Quando protegidos por TLS, conexões entre um cliente (por exemplo, um navegador da Web) e um servidor (por exemplo, wikipedia.org) devem ter uma ou mais das seguintes propriedades:

  - A conexão é *privada* (ou *segura*) porque a criptografia simétrica é usada para criptografar os dados transmitidos. As chaves para essa criptografia simétrica são geradas exclusivamente para cada conexão e são baseadas em um segredo compartilhado que foi negociado no início da sessão (Handshake TLS).

  - O servidor e o cliente negociam os detalhes de qual algoritmo de criptografia e chaves criptográficas usar antes que o primeiro byte de dados seja transmitido.

❑ TLS

- A negociação de um segredo compartilhado é segura (o segredo negociado não está disponível para bisbilhoteiros e não pode ser obtido, mesmo por um invasor que se coloque no meio da conexão) e confiável (nenhum invasor pode modificar as comunicações durante a negociação sem ser detectado).

- A identidade das partes em comunicação pode ser autenticada usando criptografia de chave pública. Essa autenticação pode ser opcional, mas geralmente é necessária para pelo menos uma das partes (geralmente o servidor).

- A conexão é confiável porque cada mensagem transmitida inclui uma verificação de integridade de mensagem usando um código de autenticação de mensagem para evitar perda não detectada ou alteração dos dados durante a transmissão.[2]

TLS

- Além das propriedades acima, a configuração cuidadosa do TLS pode fornecer propriedades adicionais relacionadas à privacidade, como sigilo de encaminhamento, garantindo que qualquer divulgação futura de chaves de criptografia não possa ser usada para descriptografar as comunicações TLS registradas no passado.

❑ TLS

- O TLS suporta muitos métodos diferentes para trocar chaves, criptografar dados e autenticar a integridade da mensagem.

- Como resultado, a configuração segura do TLS envolve muitos parâmetros configuráveis e nem todas as opções fornecem todas as propriedades relacionadas à privacidade descritas na lista.

❑ TLS

- O protocolo TLS compreende duas camadas: o registro TLS e os protocolos de handshake TLS.

- O TLS é um padrão proposto pela IETF (Internet Engineering Task Force), definido pela primeira vez em 1999, e a versão atual é o TLS 1.3 definido no RFC 8446 (agosto de 2018).

- O TLS baseia-se nas especificações SSL anteriores (1994, 1995, 1996) desenvolvidas pela Netscape Communications para adicionar o protocolo HTTPS ao navegador da Web Navigator.

❑ TLS

Descrição

Aplicações cliente-servidor fazem uso do protocolo TLS para se comunicar através de uma rede de forma a prevenir a interceptação e adulteração da informação.

Uma vez que aplicações podem se comunicar tanto através de TLS (ou SSL) como sem ele, é necessário que o cliente sinalize ao servidor para a configuração de uma conexão TLS.
Uma das maneiras de se obter isso é utilizar números de porta diferentes, por exemplo a porta 443 para HTTPS.

❑ TLS

Descrição

Outro mecanismo é uma requisição específica por parte do cliente ao servidor para uma transição para a conexão TLS; por exemplo, ao fazer uma requisição STARTTLS ao utilizar protocolos de email.

❑ TLS

- Uma vez que o cliente e o servidor concordaram quanto ao uso do TLS, eles negociam uma conexão de estado por meio de um procedimento de handshake.
- Os protocolos utilizam um handshake com uma **chave pública** para estabelecer as configurações de criptografia e uma **chave de sessão única** compartilhada através da qual toda a comunicação é criptografada utilizando uma chave simétrica.
- Durante esse handshake, o cliente e o servidor concordam a respeito dos vários parâmetros necessários para estabelecer a segurança da conexão:

TLS

- O handshake é iniciado quando o cliente se conecta a um servidor habilitado para TLS requisitando uma conexão segura e apresentando uma lista de algoritmos suportados (cifras e funções hash).

- A partir dessa lista, o servidor seleciona uma cifra e uma função hash para as quais também tenha suporte e notifica ao cliente a decisão.

- O servidor então geralmente apresenta informações de identificação na forma de um certificado digital. O certificado contém o nome do servidor, a autoridade de certificação (CA) que concedeu o certificado, e a chave pública do servidor.

- O cliente confirma a validade do certificado antes de continuar.

❑ TLS

- Para gerar as chaves de sessão utilizadas na conexão segura, o cliente:
  - criptografa um número aleatório com a chave pública recebida e envia o resultado ao servidor (o único capaz de descriptografar a mensagem com sua chave privada); ambas as partes então fazem uso do número aleatório para gerar uma chave de sessão única para a criptografia subsequente dos dados durante a sessão, ou

  - inicia uma troca de chaves de Diffie-Hellman para gerar seguramente uma chave de sessão aleatória e única, utilizada para criptografar e descriptografar os dados e que ainda possui a propriedade de *foward secrecy*: caso a chave privada do servidor seja vazada no futuro, ela é incapaz de descriptografar a sessão atual, mesmo que esta tenha sido interceptada e gravada por um terceiro.

❑ TLS

- Isso conclui o handshake e inicia a conexão segura, que é criptografada e descriptografada com a chave de sessão até o fim da conexão. **Se qualquer um dos passos acima falhar, o handshake TLS também falha e a conexão não é criada.**

BIBLIOGRAFIA

TANENBAUM, A. Redes de Computadores. Terceira Edição. Editora Campus, 2003.

SOARES, L.F.G.; LEMOS, G. e COLCHER, S. Redes de Computadores: das LANs, MANs e WANs às Redes ATM. Segunda Edição. Editora Campus. Rio de Janeiro, 1995.

KUROSE, R.. Redes de Computadores e a Internet. Quinta Edição. Editora Pearson. 2010.

TORRES, G. Redes de Computadores – Versão Revisada e Atualizada. Ed. Nova Terra, 2009.