Mecanismos de Segurança: TLS (Transport Layer Security)

Hudsson Davih
Luís Fillipe Magalhães
Nilson Deon
Sarah Magalhães

O que é o TLS?

- TLS é um protocolo de segurança que criptografa a comunicação entre dispositivos na internet.
- Seu objetivo principal é garantir confidencialidade, integridade e autenticação.
- Este protocolo está empregado principalmente na criptografia de comunicação entre navegador e servidor (HTTPS) e a proteção de emails e chamadas telefônicas (VoIP)
- Sua primeira versão foi proposta pela Força-Tarefa de Engenharia da Internet (IETF), sendo publicado em 1999.
- Sua versão mais recente é a 1.3 no qual foi lançada em 2018.

TLS ou SSL?

1. Evolução e Versões:
    - SSL foi desenvolvido pela Netscape nos anos 1990.
    - Problemas de segurança levaram à criação do TLS, iniciado como uma melhoria do SSL 3.0.
2. Criptografia e Segurança:
    - TLS oferece suporte a algoritmos mais fortes e comunicação mais segura.
    - SSL 3.0 é considerado inseguro e obsoleto.
3. Uso Moderno:
    - O termo "SSL" ainda é amplamente usado, mas o TLS é o padrão atual.
    - Recomendação: Sempre usar as versões mais recentes do TLS.

Certificado TLS

Para utilizar este mecanismo, o servidor de origem deve ter instalado um certificado TLS, esse certificado é emitido por uma autoridade de certificação, ele contém dados importantes como o proprietário do domínio e a chave pública do servidor, informações essenciais para validar a identidade do servidor

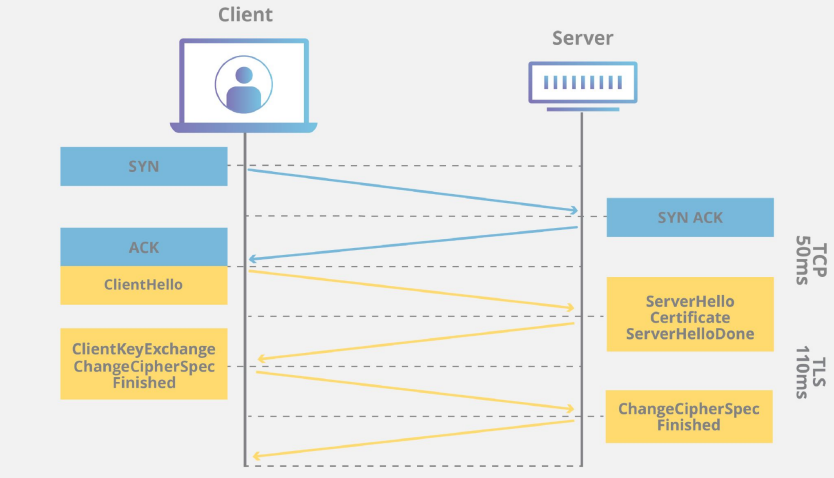
Como o TLS funciona?

1. Handshake TLS
    - Inicia a conexão entre o dispositivo cliente e servidor.
    - Define a versão do TLS e as suítes de cifras.
    - Autentica a identidade do servidor usando o certificado TLS.
    - Gera as chaves de sessão para criptografia da comunicação.
2. Pacote de Codificação:
    - Inclui algoritmos e chaves de criptografia para a sessão.
    - Utiliza criptografia de chave pública para criar um canal seguro.

Como o TLS funciona?

3. Autenticação e Integridade:

    - Certificado TLS valida a identidade do servidor.
    - Dados assinados com um autenticador de mensagem (MAC) garantem integridade e segurança, como um "lacre digital".



O que o TLS faz?

1. Proteção de Dados
    - TLS criptografa informações confidenciais, impedindo o acesso não autorizado durante a transmissão.
2. Criptografia de Ponta a Ponta
    - Apenas cliente e servidor conseguem ler as mensagens.
    - Protege contra ataques Man-In-The-Middle (MITM).
3. Autenticação e Integridade:
    - Autenticação: Verifica a identidade de servidores ou clientes usando certificados digitais confiáveis.
    - Integridade: Garante que os dados não foram alterados durante a transmissão.

O papel do TLS na segurança cibernética

1. Combinação de Criptografias
    - Simétrica: Usa uma única chave para criptografar e descriptografar (rápida e eficiente).
    - Assimétrica: Usa um par de chaves (pública e privada) para troca segura de informações.
2. Troca de Chaves Segura:
    - TLS usa criptografia assimétrica para trocar a chave simétrica de forma protegida.
    - Após a troca, a comunicação utiliza criptografia simétrica, garantindo velocidade e segurança.

O papel do TLS na segurança cibernética

3. Prevenção de MITM

    - Mesmo que os dados sejam interceptados, sem as chaves corretas eles permanecem ilegíveis.
    - Integração das duas criptografias protege contra a interceptação e manipulação dos dados.

Mas o que é o ataque MITM?

- O que é?

  Um ataque em que o invasor intercepta e manipula a comunicação entre duas partes sem que elas percebam.

- Como funciona?

  O invasor se posiciona entre o cliente e o servidor.

  Ele pode **espionar** ou **alterar dados** transmitidos.

- Consequências:

  Roubo de informações sensíveis (senhas, dados bancários).

  Manipulação de mensagens ou transações.

Questão proposta pelo grupo

Contexto:
Durante a conexão com um servidor seguro usando o protocolo TLS, o handshake TLS ocorre para estabelecer uma comunicação protegida. Um dos principais objetivos desse processo é garantir que a comunicação esteja protegida contra ataques Man-In-The-Middle (MITM).

Questão:
Qual das seguintes afirmações explica corretamente como o protocolo TLS protege contra ataques Man-In-The-Middle?

Questão proposta pelo grupo

A) O TLS usa apenas criptografia simétrica para garantir que os dados transmitidos não sejam interceptados por atacantes.

B) O TLS utiliza certificados digitais para autenticar o servidor e garantir que o cliente está se comunicando com a entidade legítima.

C) O TLS substitui a necessidade de criptografia, protegendo os dados apenas com autenticação de identidade.

D) O TLS permite que qualquer pessoa descriptografe os dados transmitidos, desde que tenha acesso à chave pública do servidor.

Questão proposta pelo grupo

Resposta correta:

B) O TLS utiliza certificados digitais para autenticar o servidor e garantir que o cliente está se comunicando com a entidade legítima.

Questão proposta pelo grupo

Justificativas:

A) Errada: Embora o TLS utilize criptografia simétrica para criptografar a comunicação após o handshake, ele também usa criptografia assimétrica e certificados digitais no início para garantir a troca segura de chaves e autenticação.

B) Correta: A autenticação por meio de certificados digitais garante que o cliente está se comunicando com o servidor correto. Isso impede ataques MITM, pois o invasor não consegue se passar pelo servidor legítimo sem o certificado digital correspondente.

Questão proposta pelo grupo

Justificativas:

C) Errada: O TLS não substitui a criptografia; ele combina criptografia com autenticação para proteger dados e prevenir manipulações.

D) Errada: A chave pública é usada para criptografar dados ou verificar assinaturas, mas não pode ser usada para descriptografar dados transmitidos. Apenas quem possui a chave privada correspondente pode fazê-lo, garantindo a confidencialidade dos dados.

Fonte

1. Cloudflare
    - Transport Layer Security (TLS) - Cloudflare
2. SSL Dragon
    - Como SSL Evita Ataques Man-In-The-Middle - SSL Dragon