HTTPS e Protocolo TLS: Uma Visão Técnica

HTTPS (Hypertext Transfer Protocol Secure)

O HTTPS é uma extensão do HTTP que adiciona segurança à comunicação entre um cliente e um servidor web.

Criptografia

O HTTPS utiliza criptografia assimétrica para proteger os dados durante a transferência.

Quando você acessa um site com HTTPS:

- O servidor envia seu certificado digital contendo sua chave pública.
- O navegador usa essa chave pública para criptografar os dados antes de enviá-los ao servidor.
- A chave privada, mantida pelo servidor, é usada para descriptografar os dados recebidos.

Certificados SSL/TLS

Os certificados digitais são emitidos por Autoridades de Certificação (CAs) e validam a identidade do servidor. Eles contêm informações como o nome do domínio, a chave pública e a assinatura digital. O navegador verifica se o certificado é válido e confiável antes de estabelecer a conexão segura.

Handshake TLS

Antes de iniciar a transferência de dados, ocorre um processo de "aperto de mãos" (handshake) entre o cliente e o servidor. Durante esse processo:

1. Cliente e servidor negociam o algoritmo de criptografia a ser usado.
2. Estabelecem uma chave de sessão para criptografia simétrica.
3. O certificado do servidor é verificado para garantir a autenticidade do servidor.

Protocolo TLS (Transport Layer Security)

O TLS é a base do HTTPS e oferece as seguintes funcionalidades:

- Criptografia Simétrica: Após o handshake inicial, uma chave de sessão é gerada e usada para criptografar e descriptografar os dados durante a comunicação.
- Criptografia Assimétrica: O handshake também envolve a troca de chaves públicas e privadas para estabelecer a criptografia simétrica.
- Integridade e Autenticidade: O TLS inclui mecanismos para verificar a integridade dos dados (através de códigos de autenticação de mensagem, MACs) e garantir a autenticidade do servidor através do certificado digital.

HTTPS impede a cópia de dados devido à segurança?

Não, o HTTPS não impede a cópia de dados. O propósito do HTTPS é garantir que a comunicação entre o cliente e o servidor seja segura. A criptografia do HTTPS protege os dados em trânsito, mas não impede que os dados sejam copiados ou armazenados uma vez que chegam ao destino final, seja no navegador do usuário ou no servidor. A cópia de dados depende das permissões e das configurações do site, não do protocolo de segurança usado.

O que o protocolo TLS faz?

O protocolo TLS protege as comunicações pela internet, criptografando os dados e garantindo sua integridade e autenticidade. Especificamente, ele:

- Criptografa os dados: Utiliza criptografia simétrica para proteger os dados durante a transmissão, garantindo que apenas as partes autorizadas possam acessá-los.
- Garante a integridade dos dados: Utiliza códigos de autenticação de mensagem (MACs) para assegurar que os dados não foram alterados durante a transmissão.
- Verifica a autenticidade do servidor: Utiliza certificados digitais para confirmar que o servidor é quem diz ser, prevenindo ataques de intermediários (man-in-the-middle).

Conclusão

O HTTPS é uma parte fundamental da segurança online. Ele protege a privacidade dos usuários e garante que suas informações não sejam interceptadas por terceiros mal-intencionados.