Victor Augusto Costa Monteiro
NºUSP 8942937
victor.augusto.monteiro@usp.br

Atividade Camada de Enlace

Redes de Computadores - ACH2026

20 de dezembro de 2023

1. Onde está implementado o SSL e como as aplicações podem utilizá-lo?

O SSL está implementado na camada de transporte. Ele serve para que, no handshake que estabelece uma conexão entre cliente e servidor, uma chave de sessão para descriptografar as mensagens que serão enviadas criptografadas entre os dois dispositivos.

2. Como o certificado do site é usado para troca de mensagens seguras no SSL e para quais mensagens?

O certificado do site serve para autenticar o servidor e possibilitar a troca segura de chaves que serão utilizadas para a criptografia dos dados durante a comunicação. A troca de chaves acontece no handshake, quando cliente e servidor estão estabelecendo uma conexão entre si.

3. Alguns dos algoritmos de criptografia usados no SSL utilizam Cypher Block Chaining. Como funciona esse mecanismo e por que protege de ataques estatísticos?

O CBC usam esquema com XOR entre textos simples e o bloco criptografado anteriormente. Basicamente cria uma dependência do bloco atual com o bloco anterior para criar uma chave em que um bloco é a chave para o bloco seguinte. Devido à dependência entre os blocos, um ataque estatístico não pode ser facilmente executado, pois mesmo pequenas alterações no texto simples resultam em mudanças significativas em todo o texto criptografado

4. O que é e como funciona a derivação de chaves no SSL?

A derivação de chaves no SSL/TLS é um processo pelo qual são geradas chaves criptográficas a partir de uma chave mestra. A chave mestra é trocada durante o handshake. A partir dela são derivadas outras chaves, que podem ser usadas em diferentes funcionalidades da aplicação, como a criptografia de pacotes e chaves de autenticação.

5. Explique que mecanismos o SSL usa para se proteger de cada um dos seguintes ataques e como esses mecanismos evitam os problemas:

a) Ataques de gravação e reprodução dentro de uma mesma sessão;

O SSL/TLS usa um mecanismo chamado MAC (Message Authentication Code) para proteger contra a modificação de dados transmitidos. O MAC é calculado usando uma chave compartilhada entre o cliente e o servidor, e é anexado a cada mensagem. Isso impede que um atacante modifique os dados sem que o destinatário perceba, já que qualquer alteração nos dados resultaria em um MAC diferente.

b) Ataques de gravação e reprodução de uma sessão inteira;

O SSL/TLS usa o conceito de nonce (número usado uma única vez) para evitar a reutilização de chaves criptográficas e evitar ataques de repetição. Os nonces são valores únicos usados em cada mensagem ou sessão, garantindo que mesmo que um conjunto de dados seja capturado, ele não possa ser reproduzido com sucesso em uma nova sessão.

c) Spoofing da mensagem pedindo para fechar a conexão;

Durante o processo de fechamento de conexão, o SSL/TLS requer um handshake para garantir a autenticidade das mensagens. Se uma mensagem de fechamento for spoofada, a parte receptora espera um processo específico de fechamento da conexão, incluindo trocas de confirmação que não podem ser facilmente falsificadas.

d) Spoofing da escolha de algoritmos de criptografia para só poder escolher os mais fracos.

O SSL/TLS tem uma lista de algoritmos suportados e preferidos. Durante o handshake, cliente e servidor negociam sobre os algoritmos a serem usados. Para mitigar esse tipo de ataque, os protocolos mais recentes e seguros do SSL/TLS são configurados para priorizar algoritmos de criptografia mais robustos e seguros, evitando que um atacante force o uso de algoritmos mais fracos.