Universidade de Brasília

Segurança Computacional
Trabalho Prático 2

Aluno

Heron Ferrari Araujo - 202063687

Departamento de Ciência da Computação

Professor(a): Lorena de Souza Bezerra Borges

Data de Entrega: 16 de Fevereiro de 2025

1 Introdução

A segurança na comunicação entre clientes e servidores na Web é um dos aspectos mais críticos da Internet moderna. O protocolo HTTPS (Hypertext Transfer Protocol Secure) desempenha um papel central ao garantir que as informações trocadas entre navegadores e servidores sejam protegidas contra ataques, interceptações e adulterações. Ele é amplamente utilizado em sites de e-commerce, serviços bancários e outras aplicações onde a privacidade e a integridade dos dados são essenciais.

O HTTPS é baseado em dois importantes protocolos de segurança: o SSL (Secure Sockets Layer) e o TLS (Transport Layer Security). Esses protocolos asseguram que a comunicação ocorra de maneira confidencial, utilizando criptografia para proteger os dados, além de autenticar as partes envolvidas e garantir a integridade das mensagens. Este trabalho tem como objetivo explorar o funcionamento do HTTPS, desde os conceitos teóricos dos protocolos SSL/TLS até a implementação prática de um cliente e servidor capazes de realizar uma comunicação segura.

A primeira parte do relatório aborda os princípios básicos de segurança implementados pelos protocolos SSL, TLS e HTTPS, destacando suas funcionalidades, os principais algoritmos envolvidos nos processos de criptografia e autenticação, e a evolução das versões desses protocolos. A segunda parte foca na implementação prática de um cliente e servidor HTTPS, utilizando bibliotecas de criptografia como OpenSSL para simular uma comunicação segura. Ao final, são apresentadas análises das comunicações realizadas, destacando o papel dos protocolos de segurança no processo.

2 Objetivos e Funcionalidades Gerais dos Protocolos

2.1 SSL (Secure Sockets Layer)

Objetivo:

O SSL foi projetado para garantir uma comunicação segura entre clientes e servidores, criando um canal criptografado que protege os dados transmitidos contra interceptação e modificação por terceiros. Ele autentica as partes envolvidas na comunicação, assegura a integridade dos dados e mantém sua confidencialidade.

Funcionalidades:

- Autenticação: O SSL usa certificados digitais para autenticar o servidor e, opcionalmente, o cliente.
- Criptografia: Protege os dados transmitidos usando algoritmos de criptografia simétrica e assimétrica.

- Integridade: Garante que os dados não sejam alterados durante a transmissão, utilizando funções de hash e códigos de autenticação de mensagem (MAC).
- Troca de Chaves Segura: Utiliza algoritmos como o RSA ou o Diffie-Hellman para realizar uma troca de chaves segura entre as partes envolvidas.

2.2 TLS (Transport Layer Security)

Objetivo:

O TLS é o sucessor do SSL e foi desenvolvido para corrigir vulnerabilidades e melhorar a segurança do protocolo. Assim como o SSL, o TLS visa garantir uma comunicação segura por meio de criptografia, autenticação e integridade dos dados, mas com mecanismos mais robustos e seguros.

Funcionalidades:

- Melhoria na Segurança: Comparado ao SSL, o TLS oferece suporte a algoritmos de criptografia mais fortes e mecanismos de verificação de integridade mais eficientes.
- Troca de Chaves Segura: TLS utiliza a troca de chaves por meio de criptografia assimétrica, garantindo que as chaves de sessão sejam trocadas de forma segura.
- Autenticação e Confidencialidade: Assim como o SSL, o TLS autentica o servidor (e, opcionalmente, o cliente) e mantém a confidencialidade da comunicação.
- Proteção Contra Ataques: TLS adiciona proteções contra ataques como o "Man-in-the-Middle"e fornece mais camadas de segurança para garantir que as sessões não possam ser interceptadas ou modificadas.

2.3 HTTPS (Hypertext Transfer Protocol Secure)

Objetivo:

O HTTPS é a versão segura do protocolo HTTP (Hypertext Transfer Protocol), utilizado para transferir dados na Web. Ele combina o protocolo HTTP com a camada de segurança fornecida pelo SSL/TLS, garantindo que as comunicações entre o navegador do cliente e o servidor sejam seguras e privadas.

Funcionalidades:

- Criptografia de Dados: HTTPS garante que todos os dados transmitidos entre o cliente e o servidor sejam criptografados, evitando que possam ser lidos por terceiros.
- Autenticação: HTTPS autentica o servidor, confirmando para o cliente que ele está se conectando ao servidor correto por meio de certificados digitais.

- Integridade dos Dados: HTTPS garante que os dados não sejam alterados ou corrompidos durante a transmissão, protegendo-os de ataques como o "Man-in-the-Middle".
- Confiança e Privacidade: HTTPS oferece uma experiência de navegação mais segura, sendo essencial para sites que manipulam dados sensíveis como informações de login, números de cartão de crédito, entre outros.

3 Implementação Prática

Nos arquivos anexados possui os códigos e um README que explica como executar o código e testar o funcionamento do cliente-servidor.

4 Conclusão

Neste trabalho, explorei o funcionamento do protocolo HTTPS e seus componentes centrais, como os protocolos SSL e TLS, essenciais para garantir a segurança das comunicações na internet. Ao analisar os mecanismos de criptografia, autenticação e integridade dos dados, pude compreender como esses protocolos asseguram que a comunicação ocorra de forma segura, protegendo informações sensíveis contra possíveis ataques.

A implementação prática de um cliente e servidor HTTPS foi uma oportunidade de aplicar os conceitos estudados em um cenário real, utilizando bibliotecas como OpenSSL para simular a comunicação segura. Através da simulação, observei o funcionamento dos protocolos de segurança em cada etapa da conexão, desde a troca de chaves até a autenticação e criptografia dos dados.

Os resultados obtidos me mostraram a importância do uso do HTTPS na web, garantindo privacidade e segurança em transações sensíveis, como operações bancárias e o envio de dados confidenciais. Essa experiência permitiu não apenas entender a eficiência dos protocolos de segurança, mas também perceber os desafios envolvidos em garantir uma comunicação robusta e confiável.

Em resumo, este trabalho contribuiu para que eu aprofundasse o entendimento da arquitetura de segurança do HTTPS e sua relevância no contexto atual da segurança da informação.