CIC0201 - Segurança Computacional – 2024/2

Profa. Lorena Borges

Trabalho de Implementação 2 – HTTPS

Este trabalho explora o funcionamento do protocolo HTTPS, responsável por implementar uma comunicação segura entre navegadores e servidores Web, através de métodos de criptografia, autenticação e integridade dos dados. Serão abordados os protocolos de segurança SSL (Secure Sockets Layer) e TLS (Transport Layer Security), enfatizando o protocolo *HTTPS over TLS* e suas principais funcionalidades de segurança.

O projeto inclui o desenvolvimento de uma pesquisa e detalhamento dos protocolos SSL/TLS e a implementação de um servidor e cliente HTTPS, simulando uma comunicação segura. Como conclusão, o projeto deverá incluir as respectivas análises das comunicações e as contribuições dos protocolos e algoritmos de segurança utilizados na comunicação segura HTTPS.

1. Pesquisa e detalhamento dos protocolos de segurança

Esta etapa do trabalho será responsável pelo detalhamento dos protocolos de segurança SSL, TLS e HTTPS. A pesquisa deverá abordar necessariamente:

- Objetivos e funcionalidades gerais de cada protocolo (não há necessidade de detalhamento para cada versão);
- Explanação das etapas de segurança e principais algoritmos envolvidos na realização dos processos de criptografia, autenticação, troca de chaves e integridade dos dados.
- Resumo das versões e evolução dos protocolos.

2. Implementação prática

Nesta parte do trabalho deverá ser elaborado o código de implementação de um servidor e cliente HTTPS. O projeto precisa incluir necessariamente:

- Os módulos cliente/servidor, detalhando as bibliotecas, protocolos e versões utilizadas;
- Testes de comunicação entre os módulos e respectivas análises, dando ênfase aos protocolos de segurança implementados.

Observações:

1. **É permitida** a utilização de bibliotecas públicas, como OpenSSL, para primitivas criptográficas de cifração e decifração simétrica, assimétrica, geração de chaves e hash.
2. A avaliação será mediante a verificação das funcionalidades e inspeção do código.
3. Implementação **preferencialmente em dupla**, podendo ser individual. Linguagens preferenciais C, C++, Java e Python.

O que deve ser entregue: o código fonte e seu executável, pesquisa e descritivo dos códigos implementados. O detalhamento das etapas dos algoritmos e protocolos de segurança envolvidos no HTTPS é de fundamental importância para a avaliação deste trabalho.

Data de Entrega: 16/02/2024. Instruções de entrega serão divulgadas oportunamente.