1. Conceitos e ferramentas utilizadas

Uma conexão utilizando o protocolo para conexões seguras SSL é sempre iniciada pelo cliente. Quando um usuário solicita a conexão com um site seguro, o navegador web (Firefox, Microsoft Edge, Opera, Chrome, etc.) solicita o envio do Certificado Digital e verifica se:

- O certificado enviado é confiável;
- O certificado é válido;
- O certificado está relacionado com o site que o enviou.

Uma vez que as informações acima tenham sido confirmadas, o navegador envia sua chave pública e as mensagens podem ser trocadas. Uma mensagem que tenha sido criptografada com uma chave pública somente poderá ser decifrada com a sua chave privada (simétrica) correspondente. Analogamente, a mensagem seria uma fechadura que possui duas chaves, umas para trancar (criptografar) e outra para destrancar (decifrar) a porta.

protocolo_SSL_ICPEdu.jpg
Imagem: Servidor web protegi

Um servidor web protegido pelo protocolo SSL utiliza o protocolo HTTPS (Hyper Text Transfer Protocol Secure), possuindo uma URL que começa em “https://", onde o S significa “secured” (seguro, protegido).

Os algoritmos de criptografia abaixo utilizam o protocolo SSL:

- DES e DAS - algoritmo de criptografia usado pelo governo americano;
- KEA - usado para a troca de chaves pelo governo americano;
- MD5 – muito usado por desenvolvedores de software para que o usuário tenha certeza que o aplicativo não foi alterado;
- RSA - Algoritmo de chave pública para criptografia e autenticação;
- SHA-1 - também usado pelo governo americano.

A versão 3.0 do SSL exige à autenticação de ambas as partes envolvidas na troca de mensagens. Ou seja, tanto cliente quanto servidor deve fazer autenticação e afirmar que são que dizem ser.

O projeto ICPEdu recomenda a ferramenta OpenSSL para a geração da Requisição de Certificado Digital. Para tanto, este guia utiliza a ferramenta OpenSSL na versão 1.1.1, versão estável presente nos repositórios padrões das distribuições Linux Debian 10 e CentOS 8.

A ferramenta OpenSSL é livre para a implementação de protocolos para Conexões Seguras SSL

(Secure Sockets Layer) e Transporte Seguro TLS (Transport Layer Security) de dados em uma rede, possibilitando a criação de certificados, chaves sumarizadas, chaves públicas e privadas e a criptografia de arquivos.

Como os certificados SSL são comumente utilizados em servidores de hospedagem web para proteção de sites corporativos, será exemplificada a instalação final dos certificados digitais em um servidor web Apache versão 2.4 em ambiente Linux Debian 10 e CentOS 8. Essa versão do Apache também está presente nos repositórios padrões de ambas as distribuições.

Revision #1
Created Wed, Sep 9, 2020 12:04 PM
Updated Fri, Oct 27, 2023 11:21 AM