UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
EAJ - ESCOLA AGRÍCOLA DE JUNDIAÍ
CURSO DE ANÁLISE E DESENVOLVIMENTO DE SISTEMAS
DISCIPLINA DE SISTEMAS DISTRIBUÍDOS

ERICK MEDEIROS DE SOUSA

RELATÓRIO SOBRE HTTPS E SSL

NATAL
Junho de 2022

ERICK MEDEIROS DE SOUSA

RELATÓRIO SOBRE ALGORITMOS GENÉTICOS

Relatório apresentado ao Curso de Análise e Desenvolvimento de Sistemas da Escola Agrícola de Jundiaí, da Universidade Federal do Rio Grande do Norte, como requisito parcial para obtenção de nota complementar na matéria de Sistemas Distribuídos, sob a orientação do Prof. Dr. Taniro Chacon Rodrigues.

NATAL
Junho de 2022

RESUMO

Neste relatório iremos apresentar de forma minuciosa e objetiva a visão adquirida do conteúdo **PROTOCOLO HTTPS E SSL**, utilizado para construção e análise de conhecimento referente a Sistemas Distribuídos e uma possível aplicação de uso relatando algumas das observações feitas.

Palavras chaves: HTTPS. SSL. Aplicações de uso.

SUMÁRIO

1. INTRODUÇÃO

Neste artigo vamos analisar em detalhes o mundo do HTTP x HTTPS, como eles funcionam e como garantir que seu site sobreviva a qualquer problema técnico ao migrar de um protocolo para outro. Esta é uma breve descrição do que vamos tratar:

No início, os profissionais de SEO usavam HTTP, um protocolo utilizado para oferecer páginas para os usuários. A Web era simples e as migrações de sites existiam apenas de domínio para domínio ou servidor para servidor. Não era necessário se preocupar com muito mais além dos redirecionamentos habituais e garantir que a migração do site fosse feita sem problemas. Depois, veio o HTTPS.

Novas tecnologias sempre criam novos problemas que devem ser resolvidos para continuar alcançando os mesmos resultados (ou melhores)

2. FUNDAMENTAÇÃO TEÓRICA

HTTP, ou protocolo de transferência de hipertexto, é a estrutura da rede mundial de computadores (“world wide web”, em inglês). É o protocolo usado pelo servidor para processar, renderizar e disponibilizar páginas da Web para o navegador do cliente. HTTP é o meio pelo qual a maior parte da Web é exibida.

HTTP e HTTPS funcionam através do que chamamos de solicitações. Essas solicitações são criadas pelo navegador do usuário quando ele interage com algum site. Esse é um elemento importante na renderização de páginas, e, sem ele, você não estaria usando a Web como ela existe hoje.

Como funciona: digamos que alguém pesquise: "como fazer a migração de um site". A solicitação é enviada para o servidor, que envia outra solicitação de volta com os resultados da consulta. Esses resultados são exibidos na SERP (página de resultados do mecanismo de pesquisa) que você vê ao concluir a pesquisa.

Tudo isso acontece em milissegundos. Essa é uma visão geral de como o protocolo de transferência de hipertexto funciona.

2.1. O que é o HTTP?

HTTP é a abreviação do protocolo de transferência de hipertexto. Esse é o principal método pelo qual os dados de páginas da Web são transferidos através de uma rede. As páginas da Web são armazenadas em servidores, que depois são disponibilizadas no computador cliente à medida que o usuário as acessa.

A rede resultante dessas conexões cria a rede mundial de computadores (world wide web) como a conhecemos hoje. Ou seja, sem HTTP, a world wide web (WWW) como conhecemos não existiria.

Uma conexão HTTP tem um grande problema: os dados transferidos através de uma conexão desse tipo não são criptografados, então você corre o risco de invasores de terceiros roubarem as informações. Todas as informações transmitidas através desta rede via HTTP não são privadas, portanto, qualquer dado de cartão de crédito e informações confidenciais não devem ser enviados se você estiver em uma página HTTP.

2.2. Como funciona o HTTPS

Ao contrário do HTTP, o HTTPS usa um certificado seguro de um fornecedor terceirizado para proteger uma conexão e verificar se o site é legítimo. Esse certificado seguro é conhecido como Certificado SSL.

SSL é a abreviação de "secure sockets layer” (camada de soquetes segura). É isso que cria uma conexão segura e criptografada entre um navegador e um servidor, que protege a camada de comunicação entre os dois.

Esse certificado criptografa uma conexão com um nível de proteção designado no momento da compra de um certificado SSL. Um certificado SSL fornece uma camada extra de segurança para dados confidenciais que você não quer que terceiros acessem. Essa segurança adicional pode ser extremamente importante quando se trata de gerenciar sites de e-commerce.

Alguns exemplos:

Quando você quer proteger a transmissão de dados de cartão de crédito ou outras informações confidenciais (como o endereço real e a identidade física de alguém).

Quando tem um site de geração de leads que depende das informações verdadeiras de alguém. Nesse caso, HTTPS deve ser usado para proteger contra ataques mal-intencionados aos dados do usuário.

O HTTPS tem vários benefícios que valem o baixo custo. Lembre-se: se não houver o certificado, um terceiro pode verificar facilmente a conexão em busca de dados confidenciais.

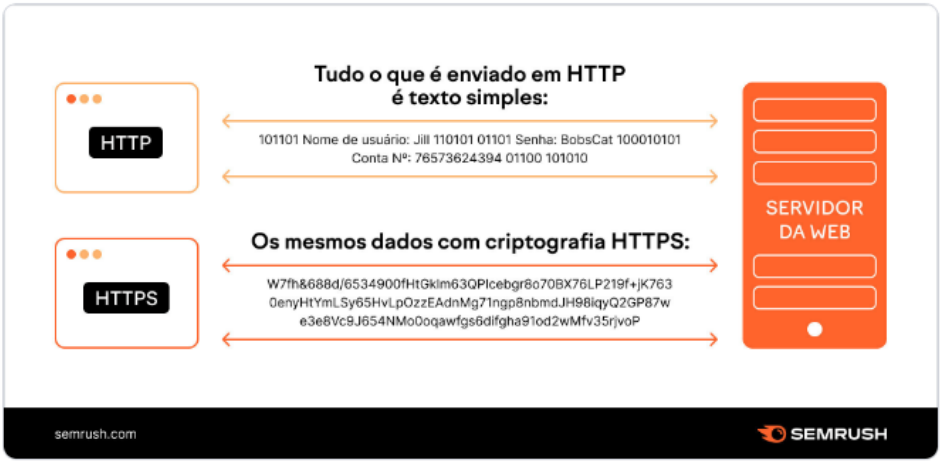

Figura 1: Sistema usando HTTPS.
Fonte: https://pt.semrush.com/blog/o-que-e-https/. Acesso em 22 de junho de 2022.

3. O QUE É SSL?

SSL significa Secure Sockets Layer, um tipo de segurança digital que permite a comunicação criptografada entre um domínio de site e um navegador. Atualmente a tecnologia se encontra depreciada e está sendo completamente substituída pelo TLS.

TLS é uma sigla que representa Transport Layer Security e certifica a proteção de dados de maneira semelhante ao SSL. Como o SSL não está mais de fato em uso, esse é o termo correto que deveria ser utilizado.

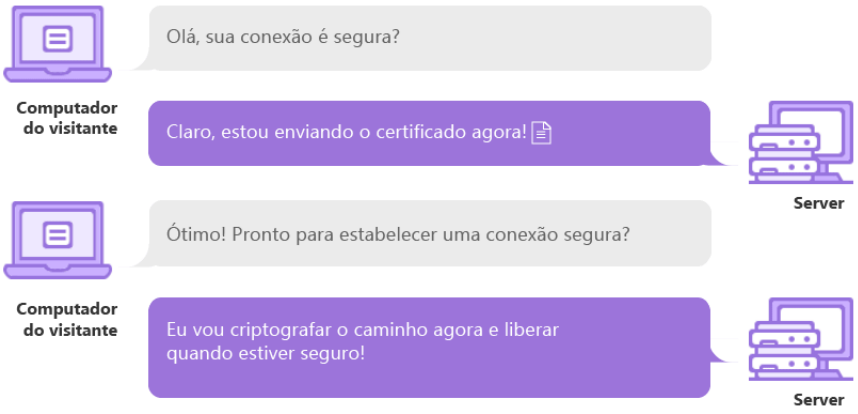

Figura 2: Exemplo de uso de SSL
Fonte: Hostinger (2022)

3.1. Como funcionam os certificados SSL/TLS?

Certificados SSL/TLS funcionam por unir digitalmente uma chave criptográfica à informação de identificação de uma companhia. Isso permite que dados possam ser transferidos de maneira que não podem ser descobertos por terceiros.

O SSL/TLS funciona através de chaves públicas e privadas, além de chaves de sessão para cada conexão segura. Quando o visitante coloca uma URL com SSL no navegador e navega pela página segura, o navegador e o servidor fazer uma conexão.

Durante a conexão inicial as chaves públicas e privadas são utilizadas para criar uma chave de sessão, que então é utilizada para criptografar e descriptografar

os dados sendo transferidos. Essa chave de sessão vai se manter válida por tempo limitado e só vai ser utilizada para essa sessão específica.

Para saber se um site utiliza a conexão SSL basta procurar por um ícone de cadeado ao lado da URL, no navegador. Ao clicar no cadeado você deve encontrar informações sobre o certificado em questão e realizar configurações.

3.2. Quando e por que é essencial ter certificado de SSL/TLS

O SSL/TLS é essencial sempre que houver informações sensíveis sendo transmitidas, como nomes de usuário, senhas e informações de pagamento.

O objetivo do SSL/TLS é garantir que somente uma pessoa – a pessoa ou organização para quem os dados estão sendo transmitidos – possa ter acesso às informações. Isso é particularmente importante quando consideramos a quantidade de dispositivos e servidores pelo qual a informação passa antes de chegar no seu destino.

Existem 3 casos onde ter um SSL/TLS é essencial:

Quando é preciso de autenticação: Qualquer servidor pode se passar por seu servidor interceptando as informações sendo transmitidas no caminho. O SSL/TLS permite que você comprove a identidade do seu servidor para que os visitantes saibam que é autêntico.

Para garantir confiabilidade: Quem possui uma loja virtual ou algum site que solicita o uso de informações pessoais é importante criar um senso de segurança para que as pessoas se sintam confortáveis em fornecer seus dados. Um certificado SSL/TLS é uma maneira visível de dizer aos seus visitantes que seus dados vão estar seguros.

Quando você precisa estar de acordo com os padrões da indústria: Em algumas indústrias, como de finanças, é necessário manter um padrão básico de segurança. Existem também algumas exigências do PCI (Payment Card Industry) para quem deseja aceitar pagamentos via cartão de crédito em seu site, e uma delas é a utilização de um certificado SSL/TLS.

É importante lembrar que o certificado SSL/TLS é válido para diversos dispositivos, o que o torna uma opção de segurança ainda mais versátil na era de dispositivos móveis. Os benefícios de ter um certificado SSL/TLS faz valer muito a pena o investimento.

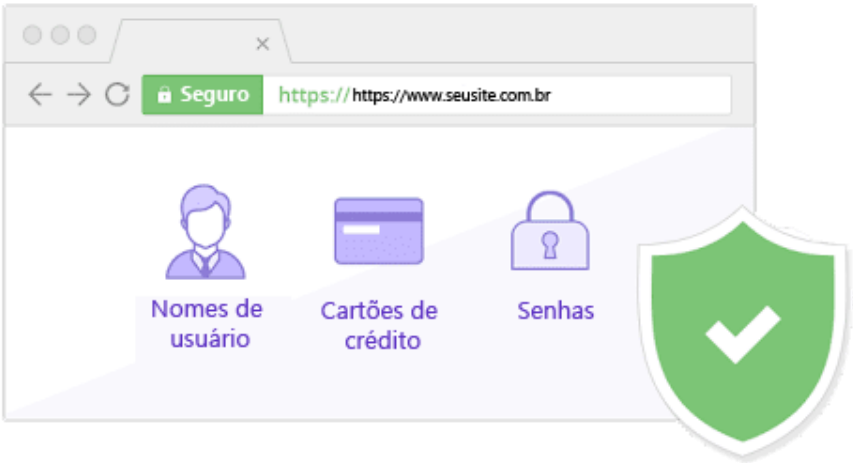

Figura 2: Exemplo de HTTPS/SSL
Fonte: Hostinger (2022)

3.3. Qual é a relação entre SSL/TLS e HTTPS?

Quando você instala um certificado SSL a transmissão de dados é configurada para ser feita via HTTPS. Ambas as tecnologias andam de mãos dadas e não funcionam uma sem a outra.

URLs são procedidas por HTTP (Hypertext Transfer Protocol) ou HTTPS (Hypertext Transfer Protocol Secure). Isso é efetivamente o que determina como qualquer dado recebido ou enviado é transmitido.

Um certificado SSL/TLS não precisa e nem deve custar uma fortuna. Você pode comprar SSL na Hostinger. Ou até conseguir um certificado SSL grátis, caso queira economizar ainda mais.

Isso significa que outra maneira de identificar se o site possui um certificado SSL é verificar que está carregando com protocolo HTTP ou HTTPS. Isso porque o protocolo HTTPS exige um certificado SSL para funcionar.

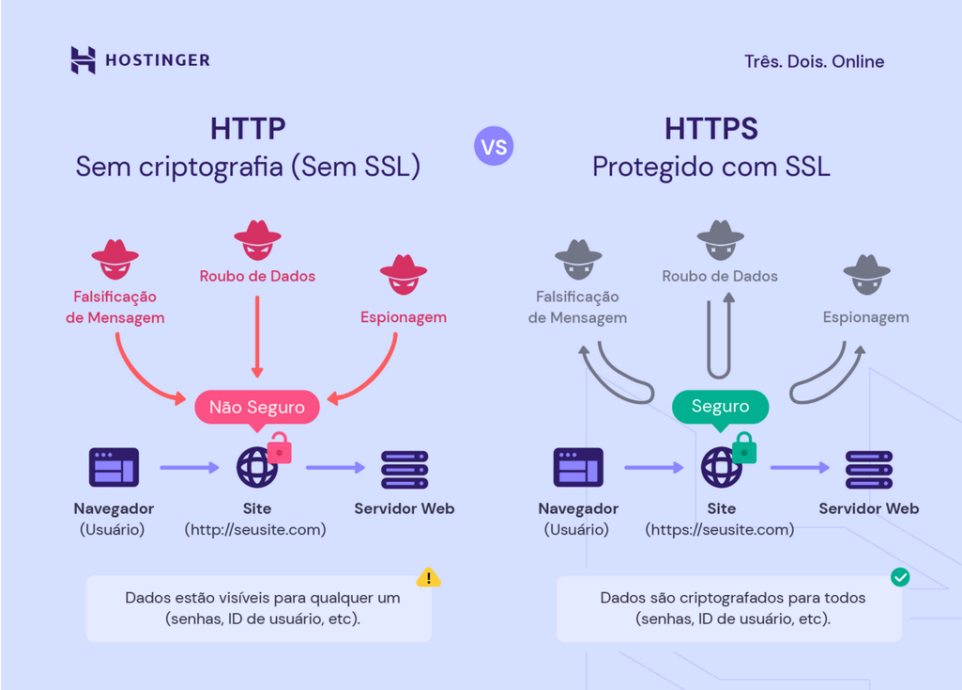

Figura 3: Exemplo de HTTPS/SSL
Fonte: Hostinger (2022)

3.4. Exemplo de aplicação de HTTPS/SSL

Para este exemplo iremos gerar um certificado local e sem validade somente para fins de teste e que pode ser utilizado no ambiente de desenvolvimento.

Para isso é necessário que tenha o openssl instalado. Depois basta executar o comando a seguir e preencher as informações necessárias.

O processo de criação consiste em ler o arquivo do certificado e a chave de acesso, subir a instancia usando o módulo HTTPS nativo do node e configurar uma porta para escutar.

```
const fs = require("fs");
const https = require("https");

// Carrega o certificado e a key necessários para a configuração.
const options = {
  key: fs.readFileSync("server.key"),
  cert: fs.readFileSync("server.cert")
};

// Cria a instância do server e escuta na porta 3000
https
  .createServer(options, (req, res) => {
    res.writeHead(200);
    res.end("Hello world using HTTPS!\n");
  })
  .listen(3000);


// Você pode testar com o curl: curl -k https://localhost:3000
// Retorno --> Hello world using HTTPS!
```

https_node_server.js hosted with ❤ by GitHub view raw

Figura 4: Criação de server HTTPS
Fonte: medium.com (2022)

Para utilizar com express basta passar a instância do express para o HTTPS depois do options.

```
const fs = require("fs");
const https = require("https");
const express = require("express");

// Instância express
const app = express();
app.get("/", (req, res) => {
  res.send("Hello world using HTTPS!");
});

// Carrega o certificado e a key necessários para a configuração.
const options = {
  key: fs.readFileSync("server.key"),
  cert: fs.readFileSync("server.cert")
};

// Cria a instância do server e escuta na porta 3000
https.createServer(options, app).listen(3000);

// Você pode testar com o curl: curl -k https://localhost:3000
// Retorno --> Hello world using HTTPS!
```

https_express_server.js hosted with ❤ by GitHub view raw

Figura 5: Criação de server HTTPS
Fonte: medium.com (2022)

Com isso já temos uma instância de servidor disponível utilizando o protocolo HTTPS, de forma prática e rápida.

CONSIDERAÇÕES FINAIS

Através deste artigo podemos observar a importância dos certificados SSL e o protocolo HTTPS, trazendo uma gama de possibilidades para a idealização dos mesmos, fazendo com que áreas do desenvolvimento como por exemplo o raciocínio, fossem exploradas através de outras metodologias e ferramentas de implementação auxiliando assim ainda mais no entendimento.

REFERÊNCIAS

HARNISH, Brian. **O que é HTTPS: guia definitivo de como funciona o HTTPS**. 2022. Disponível em: https://pt.semrush.com/blog/o-que-e-https/. Acesso em: 22 jun. 2022.

LOPES, Wesley. **Criando aplicação NodeJs com HTTPS**. 2019. Disponível em: https://medium.com/@wesdeveloper/criando-aplica%C3%A7%C3%A3o-nodejs-com-https-ce05b1d2e210. Acesso em: 22 jun. 2022.

TUPINAMBÁ, Regina. **SSL, SSH, HTTPS. O que são e para que servem?** 2014. Disponível em: https://cryptoid.com.br/ssl-tls/o-que-sao-ssl-ssh-https/. Acesso em: 22 jun. 2022.