02. A web segura - HTTPS

Date	@09/11/2022
Categoria	HTTP
Curso	HTTP: Entendendo a web por baixo dos panos

Tópicos

- HTTPS - A versão segura do HTTP
- Enviando dados com HTTP
- Funcionamento do HTTPS
- Certificado digital
- Características do HTTPS
- Autoridade certificadora
- Para Saber Mais: As chaves do HTTPS
- O que aprendemos?

Enviando dados com HTTP

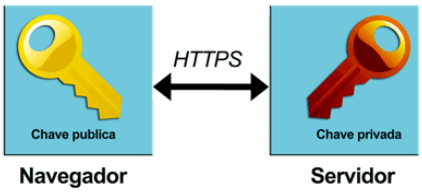
O que acontece com nossos dados quando usamos HTTP , ou seja sem a letra **S** ao final? Quando usamos HTTP, os dados são enviados em texto puro. O que pode ser perigoso, já que assim deixamos os dados abertos para intermediários.

Certificado digital

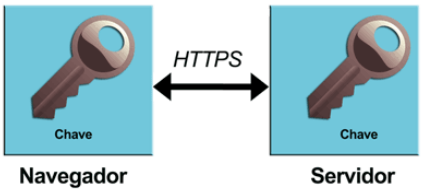
Quando precisamos informar nossos dados a algum servidor, queremos ter certeza que este servidor realmente representa a entidade em questão. Queremos confiar em quem estamos fornecendo nossos dados! Um certificado digital prova uma identidade para um site, onde temos informações sobre o seu domínio e a data de expiração desse certificado. Além disso, o certificado ainda guarda a chave pública que é utilizada para criptografar (cifrar) os dados que são trafegados entre cliente e servidor.

Para saber mais: As chaves de HTTPS

Aprendemos no vídeo que o HTTPS usa uma **chave pública** e uma **chave privada**. As chaves estão *ligadas* matematicamente, o que foi cifrado pela chave pública só pode ser decifrado pela chave privada. Isso garante que os dados cifrados pelo navegador (chave pública) só podem ser lidos pelo servidor (chave privada). Como temos duas chaves diferentes envolvidas, esse método de criptografia é chamado de **criptografia assimétrica**. No entanto, a criptografia assimétrica tem um problema, ela é **lenta**.



Por outro lado, temos a **criptografia simétrica**, que usa a mesma chave para cifrar e decifrar os dados, como na vida real, onde usamos a mesma chave para abrir e fechar a porta. A criptografia simétrica é muito **mais rápida**.



Agora, o interessante é que o **HTTPS usa ambos os métodos de criptografia, assimétrica e simétrica**. Como assim? Muita calma, tudo o que aprendemos é verdade! Só faltou o grande final :)

No certificado, vem a chave pública para o cliente utilizar, certo? E o servidor continua na posse da chave privada, ok? Isso é seguro, mas lento e por isso o cliente gera uma chave simétrica ao vivo.

Uma chave só para ele e o servidor com o qual está se comunicando naquele momento! Essa chave exclusiva (e simétrica) é então enviada para o servidor utilizando a criptografia assimétrica (chave privada e pública) e então é utilizada para o restante da comunicação.

Então, HTTPS **começa** com criptografia **assimétrica** para **depois** mudar para criptografia **simétrica**. Essa chave simétrica será gerada no início da comunicação e será reaproveitada nas requisições seguintes. Bem-vindo ao mundo fantástico do HTTPS :)

O que você aprendeu nesse capítulo?

- Por padrão, os dados são trafegados como texto puro na web.
- Apenas com HTTPS a Web é segura
- O protocolo HTTPS nada mais é do que o protocolo HTTP mais uma camada adicional de segurança, a TLS/SSL
- O tipo de criptografia de chave pública/chave privada
- O que são os certificados digitais
- Certificados possuem identidade e validade
- As chaves públicas estão no certificado, a chave privada fica apenas no servidor
- O que é uma autoridade certificadora
- O navegador utiliza a chave pública para criptografar os dados

---