David Grunheidt Vilela Ordine - 16202253

INE5429 - 2021.2 - Trabalho final em grupo

Universidade Federal de Santa Catarina

Departamento de Informática e Estatística

Ciência da Computação

Florianópolis

2021

Sumário

1 Referencial teórico

1.0.1 Certificação digital

Certificado digital pode ser considerado como a identidade eletrônica de uma pessoa ou empresa. Basicamente, ele funciona como uma carteira de identificação digital virtual, onde é possível assinar documentos a distancia com o mesmo valor judiciário de uma assinatura física.

A partir do certificado, é possível fazer uma ligação entre uma certa entidade e uma chave pública. Quando se fala de Infraestrutura de Chaves Públicas (ICP), a Autoridade Certificadora (AC) que o emite certo certificado é também responsável por assinalo. Já no caso de um modelo de Teia de Confiança (Web of trust) como o PGP, a entidade e todos os outros que confiam nela assinam o certificado. As assinaturas de ambos os exemplos são atestamentos feitos por uma entidade que confia nos dados do certificado.

No certificado é incluso, dentre outros:

- Assinatura das entidades ou ACs que validaram que a chave pública do certificado confere com as informações contidas neste.
- O período de validade do certificado.
- A chave pública associada a chave privada, a qual a segunda somente a entidade especificada no certificado possui.
- Url do "centro de revogação"(download da LCR ou para uma consulta OCSP).
- Informações sobre a entidade para o qual o certificado foi emitido (email, CPF/CNPJ, nome, PIS etc.).

1.0.2 SSL/TLS

SSL é a abreviação para *Secure Sockets Layer*, onde existe uma segurança digital que permite a comunicação criptografada entre um determinado site e um navegador. Atualmente o SSL se encontra depreciado e sendo substituido pelo TLS.

Já o **TLS** é a abreviação de *Transport Layer Security* e, semelhante ao SSL, certifica a proteção de dados.

O objetivo do SSL/TLS é tornar segura a transmissão de informações sensíveis como dados pessoais, de pagamento ou de login. Os certificados SSL/TLS funcionam através da união de uma chave criptográfica à informação de identificação de uma companhia. Assim,

dados podem ser transferidos sem serem descobertos por terceiros. Em resumo, o SSL/TLS atua através de chaves publicas e privadas, além da chave de sessão pra 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. Logo, para saber se o site usa a conexão SSL, basta procurar o ícone de cadeado ao lado da URL. Ao clicar no cadeado também é possível ver informações sobre o certificado.

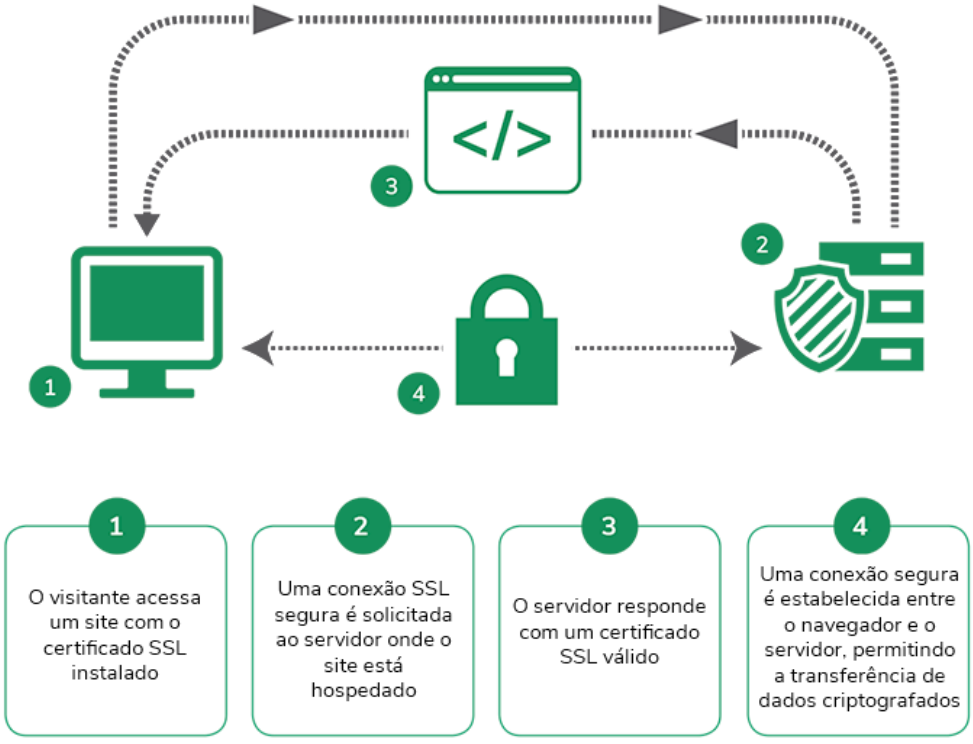


Figura 1 – Exemplo de conexão SSL/TLS

1.0.3 Projeto Let's Encrypt

A Let's Encrypt é uma autoridade certificadora gratuita, automatizada e aberta que se tornou possível graças a organização sem fins lucrativos *Internet Security Research Group* (ISRG). Seu objetivo, assim como o do protocolo ACME, é tornar possível a configuração de um servidor HTTPS e fazê-lo obter automaticamente um certificado confiável sem intervenção humana. Isso é feito através do uso do agente de gerenciamento de certificado no servidor web.

O certificado é válido por 90 dias, o qual pode ser renovado a qualquer momento. Os certificados são criados através de um processo automatizado, feito para eliminar a com-

plexidade dos processos atuais de criação, validação, instalação e renovação de certificados para sites seguros. O projeto tem como objetivo fazer com que as conexões criptografadas sejam de fácil acesso para todos os servidores da *World Wide Web*. Ao eliminar barreiras como pagamento e a renovação do certificado, espera-se que a complexidade de manter e configura a criptografia TSL diminua.

1.0.4 Protocolo ACME

O Ambiente de Gerenciamento de Certificados Automatizados (ACME) é um protocolo padrão para automatizar a validação de domínio, instalação e gerenciamento de certificados X.509. Foi projetado pelo *Internet Security Research Group* (ISRG) para seu projeto *Let's encrypt*. Em resumo, o ACME automatiza as interações entre autoridades certificadoras e os servidores web de seus usuários, permitindo assim o desenvolvimento automatizado de uma infraestrutura de chaves públicas com um custo relativamente baixo.

O ISRG fornece implementações de referência gratuitas e de código aberto para ACME: certbot é uma implementação baseada em Python do software de gerenciamento de certificados de servidor usando o protocolo ACME e boulder é uma implementação de autoridade de certificação escrita em Go. Outras implementações de servidor ACME incluem step-ca de Smallstep e Keyon Enterprise PKI.

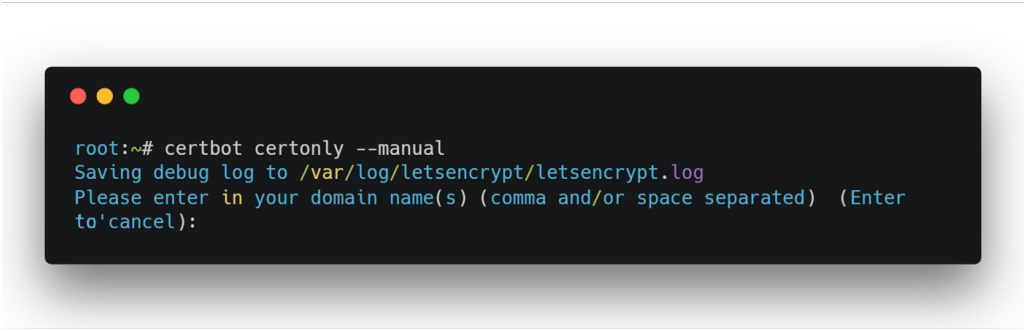
2 Primeiro experimento: Preparar um serviço de servidor Web seguro usando certificados Let's Encrypt

O experimento foi realizado através da criação de um servidor web com o auxílio dos pacotes *express* e *Node.js*. Também foi criado uma instância de uma máquina virtual (VM) com o sistema operacional (SO) *Debian 10* através do *Compute Engine*, serviço da *Google Cloud Platform* (GCP), o qual é acessível via SSH, possibilitando a execução de comandos em um terminal. Após acessar o terminal do servidor, foi feito a atualização das informações dos pacotes do SO e, na sequência, instalados as ferramentas NVM, npm, Express, *Node.js* e *Certbot*.

O *Certbot* é uma ferramente gratuita e *open-source* usada para habilitar HTTPS em websites, de forma automática, usando os certificados *Let's Encrypt*. Essa ferramenta foi usada para geração do certificado SSL. Para isso, foi executado o seguinte comando:

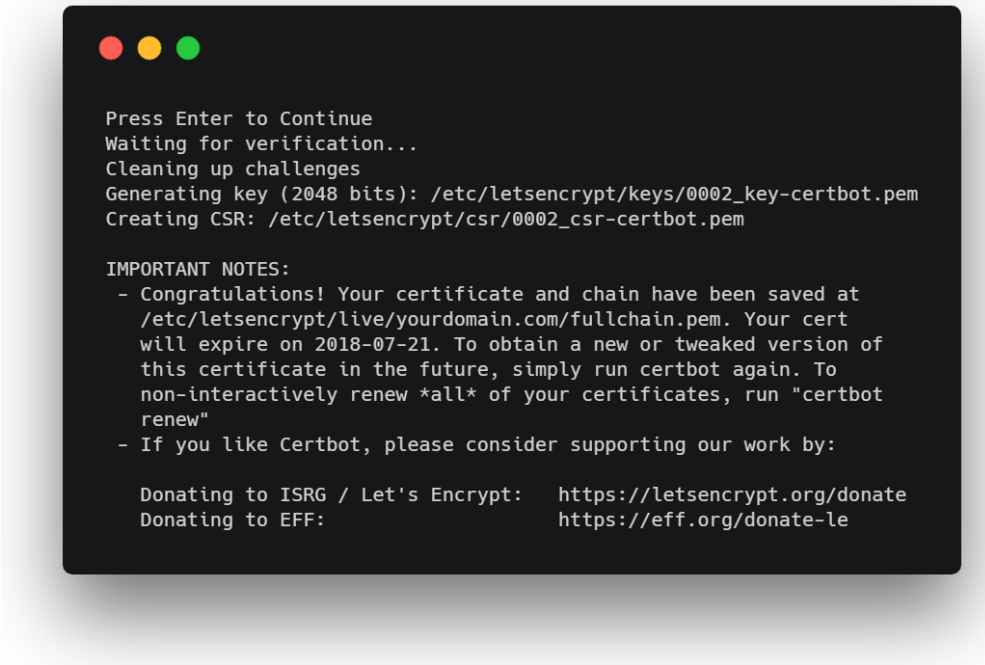
```
$ sudo certbot certonly ––manual
```

O terminal então pede para informar um domínio:



E após isso irá pedir a criação de um arquivo chamado *a-string* com o conteúdo *a-challenge*. É necessário criar os diretórios a partir da pasta raiz do servidor. Estes dois nomes acima são só exemplos do que será informado na hora da criação.

Após a criação do arquivo, o IP externo da VM em questão foi associado ao domínio **trabgrupotlsine.zapto.org**, criado a partir do site noip.com, tornando possível o acesso ao arquivo. Dando continuidade, com a ajuda do *Express* e *Node.js* criou-se um servidor mínimo para tornar possível o acesso a este arquivo. Somente após subir o servidor é que houve a continuação da configuração do certificado SSL via *certbot*. Ao final, é mostrado uma mensagem de sucesso:



Ao final, acessando o site https:// trabgrup otlsine.zapto.org é possível ver o ícone de cadeado ao lado da *url*, mostrando que a conexão via HTTPS foi feita. O certificado criado para este experimento pode ser conferido através do link https://www.ssllabs.com/ssltest/analyze.html?d=trabgrupotlsine.zapto.org.

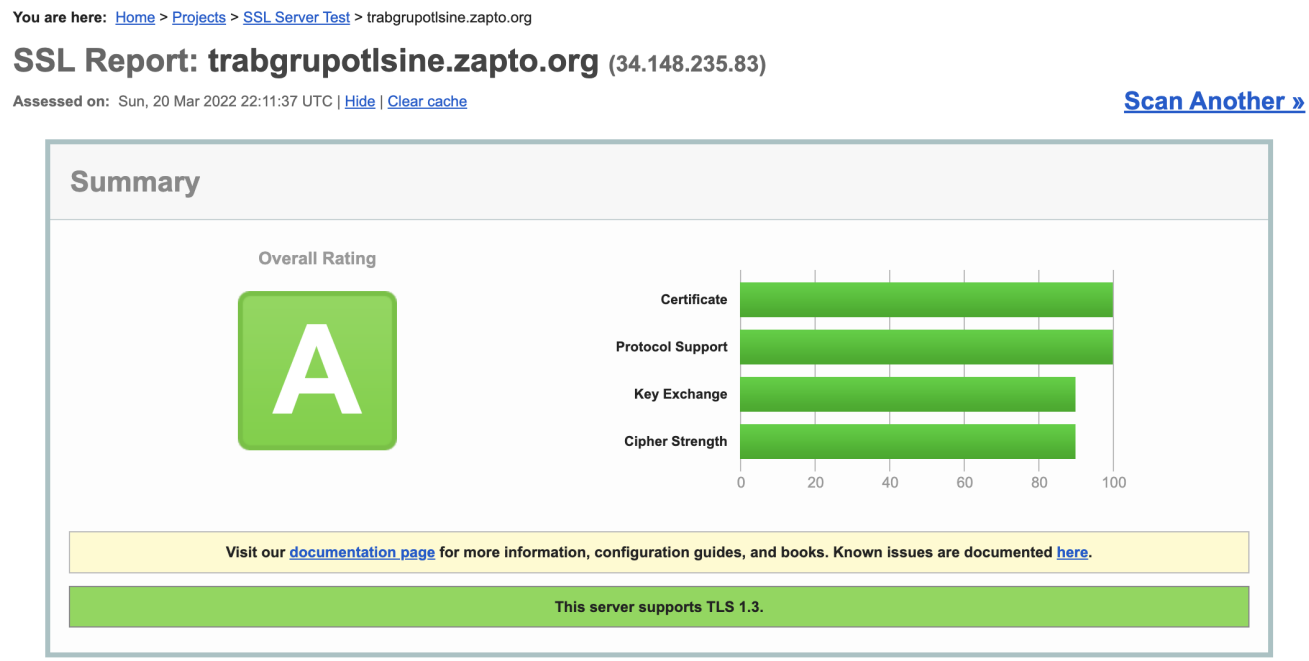


Figura 2 – Verificação do SSL no domínio do exemplo

3 Segundo experimento: Preparar um serviço proprietário para a renovação automática de certificados TLS proprietários

Infelizmente não foi possível realizar o segundo experimento por problemas pessoais e profissionais do autor deste trabalho.