CST em Análise e Desenvolvimento de Sistemas — Prof. Emerson Ribeiro de Mello
SEG786203 – Segurança da Informação — mello@ifsc.edu.br

Laboratório 2: certificados digitais

05/11/2024

Nesse laboratório serão demonstrados os passos para subir um servidor *web* Nginx e configurado com certificados digitais autoassinados para HTTPS. No segundo exemplo será feito uso de certificados digitais assinados por uma Autoridade Certificadora (CA). No terceiro exemplo é demonstrado como trabalhar com certificados digitais em projetos Java, usando o Java Keytool e *keystores*.

1 Criando certificados digitais autoassinados

Os passos a seguir mostram como gerar um certificado digital autoassinado e configurar o servidor *web* Nginx para usar HTTPS. Faremos uso de um contêiner Docker para subir o servidor *web* Nginx. Iremos fazer o mapeamento das portas HTTP (80) e HTTPS (443) do contêiner para as portas 8080 e 8443 do hospedeiro, respectivamente.

1. Criação da chave privada do servidor

```
# Criação de diretórios para armazenar os certificados e chaves do servidor
mkdir -p ~/primeiro/ssl/{certs,private} && cd ~/primeiro/ssl

# Criação da chave privada do servidor
openssl genrsa -out private/server.key 2048
```

2. Criação do certificado autoassinado do servidor

```
# Criação do certificado autoassinado
# Será necessário informar o FQDN (Fully Qualified Domain Name) do servidor, por exemplo,
    servidor.com.br no campo CN
# Neste exemplo usaremos localhost como FQDN do servidor pois acessaremos o servidor via
    localhost da máquina hospedeira
openssl req -x509 -new -key private/server.key -out certs/server.crt -days 365 -subj "/C=BR/
    ST=SC/L=Sao Jose/O=IFSC/OU=SEG/CN=localhost"

# Exibindo o conteúdo do certificado
openssl x509 -in server.crt -text -noout
```

1.1 Uso de certificados digitais em um servidor web Nginx

Crie a seguinte estrutura de diretórios e arquivos no seu diretório de trabalho.

```
primeiro
|-- Dockerfile
|-- html
|   `-- index.html
|-- nginx.conf
`-- ssl
    |-- certs
    `-- private
```

O arquivo `Dockerfile` (veja Listagem 1) contém as instruções para criar a imagem do Nginx. O arquivo `nginx.conf` (veja Listagem 2) contém a configuração do servidor Nginx com suporte a HTTP e HTTPS e o arquivo `index.html` será a página inicial do servidor Nginx.

Listagem 1: Conteúdo do arquivo `Dockerfile`

```
FROM nginx:alpine

COPY ssl /etc/nginx/
COPY nginx.conf /etc/nginx/conf.d/default.conf
```

Listagem 2: Configuração de certificados no Nginx

```
server {
    listen 80 default_server;
    listen [::]:80 default_server;
    listen 443 ssl default_server;
    listen [::]:443 ssl default_server;

    server_name localhost;

    ssl_certificate      /etc/nginx/certs/server.crt;
    ssl_certificate_key  /etc/nginx/private/server.key;

    location / {
        root /usr/share/nginx/html;
        index  index.html index.htm;
    }
}
```

Agora é necessário criar a imagem do Nginx com a configuração acima e executar o contêiner.

```
# Criar a imagem do Nginx
docker build -t nginx-ssl .

# Executar o contêiner do Nginx fazendo o mapeamento das portas 80 e 443 do contêiner
docker run -it -p 8080:80 -p 8443:443 -v $(pwd)/html:/usr/share/nginx/html --rm nginx-ssl
```

Para acessar o servidor Nginx, via HTTP, abra o navegador e acesse http://localhost:8080 ou https://localhost:8443, para acessar o servidor via HTTPS. Acessando via HTTPS o navegador irá exibir um aviso de que a conexão não é segura, pois o certificado é autoassinado.

2 Certificados digitais assinados por uma Autoridade Certificadora

Nessa seção é demonstrado como gerar chave privada e certificado digital autoassinado de uma Autoridade Certificadora (CA). Uma vantagem de usar certificados assinados por uma CA é que o navegador não exibirá um aviso de segurança ao acessar o servidor via HTTPS, se a CA estiver na lista de autoridades confiáveis do navegador.

1. Criação da chave privada da Autoridade Certificadora (CA)

```
# Criação de diretórios para armazenar os certificados e chaves da CA
mkdir -p ~/ca/{certs,private} && cd ~/ca

# Criação da chave privada da Autoridade Certificadora (CA).
# Forneça uma senha com pelo menos 4 caracteres
openssl genrsa -aes256 -out private/ca.key 4096
```

2. Criação do certificado autoassinado da Autoridade Certificadora (CA)

```
# Criação do certificado autoassinado da Autoridade Certificadora (CA)
openssl req -new -x509 -days 365 -key private/ca.key -out certs/ca.crt -subj "/C=BR/ST=SC/L=
    Sao Jose/O=IFSC/OU=SEG/CN=CA"
```

3. Criação da chave privada do servidor

```
# Criação de diretórios para armazenar os certificados e chaves do servidor
mkdir -p ~/segundo/{certs,private} && cd ~/segundo

# Criação da chave privada do servidor
openssl genrsa -out private/segundo.key 2048
```

4. Criação do pedido de certificado (CSR, *Certificate Signing Request*) do servidor para ser assinado pela CA

```
# Será necessário informar o FQDN (Fully Qualified Domain Name) do servidor, por exemplo,
    servidor.com.br no campo CN
openssl req -new -key private/segundo.key -out segundo.csr -subj "/C=BR/ST=SC/L=Sao Jose/O=
    IFSC/OU=SEG/CN=localhost"
```

5. Assinatura do CSR com a chave privada da CA e criação do certificado do servidor

```
# Assinatura do CSR com a chave privada da CA
openssl x509 -req -days 365 -in segundo.csr -CA ~/ca/certs/ca.crt -CAkey ~/ca/private/ca.key
     -CAcreateserial -out certs/segundo.crt

# Exibir o conteúdo do certificado
openssl x509 -in certs/segundo.crt -text
```

6. Verificar a cadeia de certificados

```
verify -CAfile ~/ca/certs/ca.crt ~/segundo/certs/segundo.crt
```

Se você deseja usar o certificado do servidor no Nginx, siga os passos descritos na seção anterior, substituindo o certificado autoassinado pelo certificado assinado pela CA.

3 Java Keytool e keystores

O Java Keytool é uma ferramenta, fornecida com o JDK, para gerenciar chaves e certificados digitais em um *keystore*. O *keystore* é um repositório de chaves e certificados digitais que pode ser usado em aplicações Java. Servidores de aplicação Java, como Apache TomCat, Jetty, WildFly, entre outros, usam *keystores* para armazenar chaves privadas e certificados digitais para uso em conexões seguras (HTTPS).

3.1 Criar um *keystore* com o Java Keytool

Listagem 3: Criar um *keystore* com uma chave privada e um certificado autoassinado

```
keytool -genkey -alias servidor -keyalg RSA -keysize 2048 -keystore servidor.jks -storepass
    minhasenha -keypass minhasenha -dname "CN=servidor, OU=SEG, O=IFSC, L=Sao Jose, ST=SC, C=BR"
```

- `-genkey`: gera um par de chaves pública/privada;
- `-alias servidor`: nome do alias para a chave privada;
- `-keyalg RSA`: algoritmo de criptografia RSA;

- `-keysize 2048`: tamanho da chave RSA de 2048 bits;
- `-keystore servidor.jks`: nome do arquivo de *keystore*;
- `-storepass minhasenha`: senha do *keystore*;
- `-keypass minhasenha`: senha da chave privada;
- `-dname`: campos do certificado (CN=servidor, OU=SEG, O=IFSC, L=Sao Jose, ST=SC, C=BR).

3.2 Exibir o conteúdo do *keystore*

```
# Exibir o conteúdo do \textit{keystore}
keytool -list -keystore servidor.jks -storepass minhasenha

# Exibir o conteúdo do certificado do  alias servidor
keytool -list -v -alias servidor -keystore servidor.jks -storepass minhasenha
```

3.3 Exportar o certificado do *keystore*

É possível exportar o certificado do *keystore* para um arquivo `.cer` que pode ser importado em outros *keystores* ou navegadores.

```
keytool -export -alias servidor -file servidor.crt -keystore servidor.jks -storepass minhasenha
```

3.4 Importar um certificado em um *keystore*

```
# Importar o certificado de uma Autoridade Certificadora (CA) em um \textit{keystore}
keytool -importcert -alias ca-raiz -file ca-cert.pem -keystore servidor.jks -storepass minhasenha

# Importar o certificado do servidor em um \textit{keystore}
keytool -importcert -alias servidor -file servercert.crt -keystore servidor.jks -storepass
    minhasenha
```

3.5 Remover um certificado de um *keystore*

```
# Remover o certificado do servidor do \textit{keystore}
keytool -delete -alias servidor -keystore servidor.jks -storepass minhasenha
```

4 Configurar o keytore em um projeto Java com Spring Boot

Após criar o *keystore* com a chave privada e o certificado autoassinado, você pode configurar o *keystore* no projeto Spring Boot[1] para usar HTTPS. Vamos criar um projeto Spring Boot com o Spring Initializr[2] e configurar o *keystore* no arquivo `application.properties` do projeto.

Para criar um projeto Spring Boot com o Spring Initializr, acesse o site https://start.spring.io e adicione a dependências `Spring Web`. Após baixar o ZIP com o projeto, descompacte o arquivo e adicione o arquivo `servidor.jks` (criado com o comando apresentado na Listagem 3) no diretório `src/main/resources` do projeto. E adicione as seguintes configurações no arquivo `src/main/resources/application.properties`:

[1] https://spring.io
[2] https://start.spring.io

```
server.port=8443
server.ssl.key-store=classpath:servidor.jks
server.ssl.key-store-password=minhasenha
server.ssl.key-store-type=JKS
server.ssl.key-alias=servidor
server.ssl.key-password=minhasenha
```

Por fim, crie um controlador para testar a aplicação. O código do controlador está no Listagem 4. Para executar o projeto, execute o comando `gradle bootRun` e acesse a aplicação em https://localhost:8443.

Listagem 4: Classe `TestController.java`

```
package com.example.demo;

import org.springframework.web.bind.annotation.GetMapping;
import org.springframework.web.bind.annotation.RequestMapping;
import org.springframework.web.bind.annotation.RestController;

@RestController
@RequestMapping("/")
public class TestController {

    @GetMapping
    public String test() {
        return "Hello World!";
    }
}
```