Certificados digitais

Esta prática de laboratório visa explorar o uso de certificados digitais X.509 no âmbito da Web.

Explorando certificados

Acesse os sites Web da lista abaixo e analise os certificados que eles oferecem ao navegador:

- https://carrinho.americanas.com.br
- https://sites.google.com
- https://listas.inf.ufrgs.br

Para cada site acessado, responda às seguintes questões:

- quem emitiu o certificado?
- qual o período de validade do certificado?
- qual a finalidade do certificado (conforme informado no campo de extensão `Key Usage`, se estiver presente)?
- qual a cadeia de certificação estabelecida?

Explorando a cadeia de certificação

O utilitário OpenSSL oferece várias funcionalidades para trabalhar com certificados SSL/TLS. Por exemplo, o comando abaixo permite visualizar a cadeia de certificação de um determinado serviço de rede:

```
openssl s_client -showcerts -connect www.server.com:port_number
```

Usando esse programa, analise a cadeia de certificação dos sites indicados no exercício anterior. Existem informações que não haviam sido encontradas anteriormente?

Criando uma CA e assinando certificados

Este roteiro (adaptado deste site) compreende a criação dos arquivos básicos que definem uma Autoridade Certificadora (CA) e do seu uso para assinar digitalmente o certificado de um site Web seguro.

Na CA

Criar a estrutura de diretórios e arquivos usados pela CA, de acordo com os valores *default* definidos em `/usr/lib/ssl/openssl.cnf`:

```
mkdir demoCA demoCA/private demoCA/newcerts
touch demoCA/index.txt
echo "01" > demoCA/serial
```

Gerar o certificado digital de nossa CA “raiz” (auto assinado), com validade (por exemplo) para 10 anos:

```
openssl req -new -x509 -out certificate.pem -days 3650
```

O certificado é gerado em no formato PEM (*Privacy Enhanced Mail*). Pode-se visualizar o conteúdo do certificado recém gerado em um formato textual usando:

```
openssl x509 -inform pem -in certificate.pem -text
```

A seguir, mover o certificado e a chave privada da CA para os locais adequados:

```
mv certificate.pem demoCA/cacert.pem
mv privkey.pem demoCA/private/cakey.pem
```

No servidor Web

Inicialmente, gerar um **certificado auto-assinado** para o site Web seguro:

```
openssl req -nodes -new -x509 -keyout site_privkey.pem -out site_certif_self.pem -
days 365
```

O certificado auto-assinado `site_certif_self.pem` e sua respectiva chave privada `site_privkey.pem` gerados nesta etapa poderiam ser usados na configuração de um site Web auto-certificado. Um site auto-certificado oferece comunicação segura do ponto de vista da confidencialidade, mas sua autenticidade não pode ser confirmada pelo cliente.

A partir do certificado auto-assinado, deve ser gerada uma **requisição de assinatura de certificado**, a ser enviada à CA:

```
openssl x509 -x509toreq -in site_certif_self.pem -signkey site_privkey.pem -out
site_request.pem
```

O arquivo `site_request.pem` será enviado à CA para ser assinado digitalmente. Esse envio pode ser feito por e-mail ou outro meio, mesmo que não seguro.

Na CA

Quando a CA recebe a requisição de assinatura de certificado, ela o assina usando sua chave privada e seu próprio certificado:

```
openssl ca -policy policy_anything -out site_certif_signed.pem -infiles
site_request.pem
```

O certificado do site assinado pela CA pode ser visualizado através do seguinte comando:

```
openssl x509 -inform pem -in site_certif_signed.pem -text
```

A CA então envia o certificado assinado por ela (`site_certif_signed.pem`) de volta para o site Web.

No servidor Web

Os arquivos `site_certif_signed.pem` (certificado assinado pela CA) e `site_privkey.pem` (chave privada do site) podem então ser **instalados no servidor Web**, de acordo com a configuração de cada servidor. Os

arquivos `site_certif_self.pem` e `site_request.pem` podem ser descartados, pois não têm mais utilidade.

Sugestões de servidores Web para testar o certificado: Apache, Lighttpd e NGinx.

No navegador (cliente)

- Acesse o servidor Web seguro a partir de outra máquina. O que aconteceu?
- Para que o navegador aceite o certificado do site Web seguro, ele deve ter o certificado da entidade certificadora (CA) armazenado em sua base de certificados. Por isso, inclua o certificado de nossa CA (arquivo `demoCA/cacert.pem`) no repositório de certificados do navegador.
- Acesse novamente o servidor Web seguro. Mudou algo?