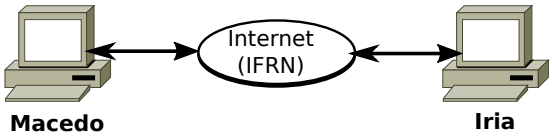
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Segurança de Rede
Prática 18: Assinatura e Certificado Digital com OpenSSL.

Olá, meus alunos!! Como é que vocês vão? Na aula de hoje iremos compreender na prática como funciona assinatura e certificado digital. Utilizar o OpenSSL para gerar pares de chaves, certificados e realizar verificação de assinaturas. Exploraremos o uso de criptografia assimétrica na verificação de autenticidade, integridade e não repúdio. Vamos lá!!! Preparados???

Configurando o Ambiente

Para estudarmos estes conceitos e ferramenta iremos utilizar duas máquinas virtuais. Uma para transmitir os segredos (Iria) e outra para receber os segredos (Macedo). Podemos utilizar qualquer distribuição Linux. Nos nossos testes utilizei Kali Linux (máquina de Iria) e uma máquina Ubuntu (máquina Macedo), ambas configuradas em Rede Nat.



Assinatura Digital

Na aula passada, aprendemos que o HMAC (Código de Autenticação de Mensagens baseada em Hash) garante a integridade e autenticidade das mensagens utilizando a função hash com chave simétrica. Entretanto, temos o problema de distribuição das chaves simétricas. Visando solucionar esta problemática surgiu o conceito de assinatura digital.

A assinatura digital é um recurso criptográfico utilizado para garantir a autenticidade, a integridade e o não repúdio de uma informação digital. Por meio dela, é possível assegurar que uma mensagem ou documento eletrônico foi realmente criado pelo remetente declarado (autenticidade), que seu conteúdo não foi alterado desde que foi assinado (integridade) e que o autor da assinatura não possa negar sua autoria posteriormente (não repúdio).

O funcionamento da assinatura digital baseia-se na criptografia assimétrica, que utiliza um par de chaves: uma chave privada, conhecida apenas pelo remetente, e uma chave pública, que pode ser compartilhada com qualquer pessoa. Para assinar digitalmente um documento, o remetente gera um resumo (ou hash) do conteúdo e, em seguida, criptografa esse hash com sua chave privada. O resultado é a assinatura digital.

A assinatura digital é uma forma de autenticação eletrônica que utiliza criptografia de chave pública e hash para garantir a integridade e a autenticidade de um documento ou mensagem digital. Ela funciona como uma assinatura manuscrita, mas com muito mais segurança e validade jurídica em transações eletrônicas.

Ao receber o documento e a assinatura, o destinatário pode verificar a validade da assinatura. Para isso, ele gera novamente o hash do documento recebido e descriptografa a assinatura utilizando a chave pública do remetente. Se os dois valores coincidem, isso indica que o documento não foi alterado e que a assinatura foi feita pela pessoa que detém a chave privada correspondente à chave pública usada na verificação.

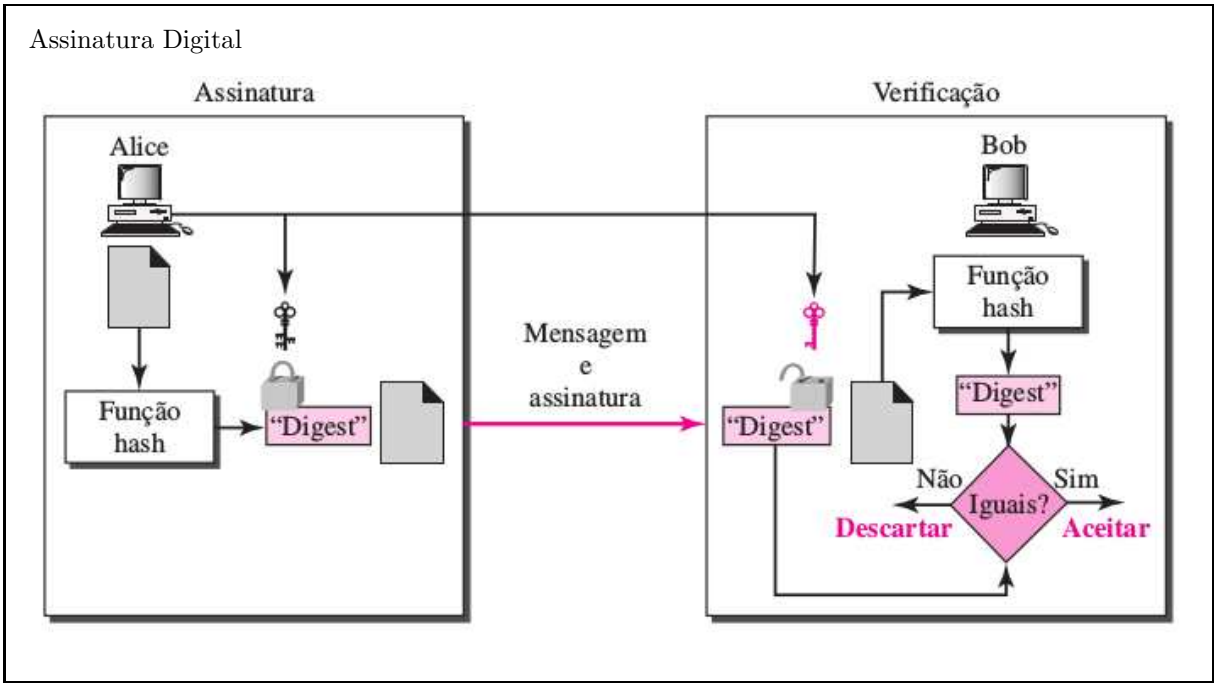
A assinatura digital é amplamente utilizada em sistemas eletrônicos, como notas fiscais eletrônicas, autenticação de e-mails, contratos digitais e sistemas governamentais que exigem segurança e confiabilidade nas comunicações.

Certificado Digital

O certificado digital é um documento eletrônico que funciona como uma identidade virtual, associando uma chave pública criptográfica a uma pessoa, organização ou sistema. Ele pode ser emitido pela própria pessoa (certifcado autoassinado) ou emitido por uma Autoridade Certificadora (AC). A Autoridade Certificadora é uma entidade confiável responsável por validar a identidade do solicitante e garantir que aquela chave pública realmente pertence a quem diz ser o seu dono.

O funcionamento do certificado digital baseia-se na criptografia assimétrica, que utiliza um par de chaves: uma chave privada, que deve ser mantida em segredo, e uma chave pública, que pode ser compartilhada livremente. O processo inicia-se com a geração desse par de chaves. Em seguida, o solicitante envia sua chave pública, junto com seus dados pessoais ou organizacionais, para a Autoridade Certificadora, por meio de uma Solicitação de Assinatura de Certificado (CSR). Após validar as informações, a AC emite o certificado digital, assinando digitalmente o documento com sua própria chave privada.

Assinatura Digital



O certificado emitido contém informações como o nome do titular, sua chave pública, o período de validade, o nome da Autoridade Certificadora e a assinatura digital da AC. Qualquer pessoa que receba um certificado assinado por Entidades pode verificar sua autenticidade utilizando a chave pública da AC, que geralmente já está instalada em navegadores e sistemas operacionais confiáveis. Essa cadeia de confiança permite que usuários se comuniquem com segurança, troquem documentos assinados digitalmente e validem identidades na internet.

OpenSSL

OpenSSL, já utilizado em aulas passadas, é uma poderosa ferramenta de código aberto que implementa os protocolos SSL (Secure Sockets Layer) e TLS (Transport Layer Security), além de oferecer uma ampla gama de funções de criptografia. Ela permite realizar operações como geração de chaves, criação de certificados digitais, assinatura e verificação de dados, criptografia de arquivos, entre outras.

Iremos utiliza-la para gerar chaves criptográficas, assinar documentos, gerar certificados digitais e verificar a assinatura digital. Para isso, siga os seguintes passos:

1. Gerar par de chave privada com o RSA que será usada para assinar digitalmente o documento e para criar o certificado.

```
openssl genpkey -algorithm RSA
 -out chave_privada.pem
```

Esse comando cria um arquivo chamado chave_privada.pem, contendo uma chave privada. Esta chave deve ser mantida em sigilo absoluto, pois ela garante a identidade do emissor.

2. Criar um texto simples que representará o conteúdo a ser assinado.

```
echo "texto para assinar" > mensagem.txt
```

O conteúdo do arquivo pode ser qualquer texto, contrato ou mensagem importante.

3. Gerar a assinatura digital do documento.

```
openssl dgst -sha256
 -sign chave_privada.pem
 -out assinatura.bin mensagem.txt
```

É calculado um resumo criptográfico (hash) do documento e, em seguida, esse resumo é criptografado com a chave privada. O resultado é salvo em um arquivo chamado assinatura.bin.

4. Exportar a chave pública:

```
openssl rsa -pubout
 -in chave_privada.pem
 -out chave_publica.pem
```

A chave pública RSA é extraida e colocada no arquivo chave_publica.pem.

5. Gerar uma solicitação de Certificado

```
openssl req -new -key
 chave_privada.pem -out requisicao.csr
```

O certificado digital associa a identidade do emissor à sua chave pública. Para essa simulação, criaremos um certificado autoassinado (sem envolvimento de uma Autoridade Certificadora externa). Durante o processo, o sistema pedirá algumas informações como o nome do emissor, e-mail, país, e outros dados de identificação. Inicialmente iremos criar a requisicao para um certificado autoassinado.

6. Gerar o certificado autoassinado

```
openssl x509 -req -in requisicao.csr
 -signkey chave_privada.pem
 -out certificado.crt
```

O certificado será salvo no arquivo certificado.crt.

7. O emissor deve enviar ao receptor três arquivos: O documento original (mensagem.txt), a assinatura digital (assinatura.bin) e o certificado digital (certificado.crt).

8. Cliente deverá extrair a chave pública do certificado digital.

```
openssl x509 -in certificado.crt
 -pubkey -noout > chave_publica_extraida.pem
```

O comando acima gera o arquivo chave_publica_extraida.pem, contendo a chave pública do emissor. Essa chave será usada para verificar a assinatura digital.

9. Cliente verifica a assinatura

```
openssl dgst -sha256 -verify
 chave_publica_extraida.pem
 -signature assinatura.bin mensagem.txt
```

Com a chave pública extraída, a assinatura e o documento original, o receptor pode verificar se o conteúdo foi assinado corretamente:

- Se o conteúdo não foi alterado e a assinatura foi feita com a chave privada correspondente à chave pública extraída, o terminal exibirá: Verified OK.
- Caso o conteúdo do arquivo tenha sido modificado ou a assinatura não seja válida, será exibido: Verification Failure.

Atividades

01. Crie um arquivo de texto, chamado mensagem.txt com o seu nome e sua matrícula. Gere sua chave de assinatura, assine digitalmente o arquivo e gere um certificado digital autoassinado. Envie pelo Google Sala de Aula: o arquivo de texto (mensagem.txt), a sua assinatura em cima do arquivo e o seu certificado digital.

02. Vertifique o que aconteceria se o arquivo mensagem.txt fosse alterado após a assinatura?

03. Qual a importância do certificado digital nesse processo?

04. Por que a função hash é utilizada na criação da assinatura digital? Qual sua importância?