Segurança em Computação
Trabalho Individual III

João Paulo Taylor Ienczak Zanette

30 de abril de 2019

Parte 1. Introdução a PGP/GPG

1. Criar certificado PGP. Obs: salvar a chave privada e não esquecer senha.
Faça um backup da sua chave privada; Publicar a chave pública em um repositório GPG.
Exemplos:

- Keyserver da RNP (use o Google para encontrar o site)
- MIT PGP Public Key Server
- Keyserver PGP.com

Resultado Esperado:

☑ Certificado do aluno publicado no repositório PGP.

Parte 2. Revogação de Certificado

2. Crie um novo certificado GPG para este trabalho individual (Não use o seu certificado pois este novo será revogado). Coloque esse certificado de testes no servidor GPG. Depois verifique seu status. Então, crie um certificado de revogação e revogue o certificado de testes.
Resultado Esperado:

☑ Faça um relatório do que você fez, incluindo o KeyID do certificado revogado.

Primeiramente, foi criada a chave GPG exatamente da mesma forma que foi feito para a Parte 1, ou seja, a partir da linha de comando foi executado:

```
$ gpg --full-generate-key  # Geração da chave
$ gpg --armor --export 5B1B5A3BD6CEE72D # Mostrar a chave pública no terminal
```

Em seguida, no site do servidor de chaves da RNP foi adicionada, podendo ser buscada em `http://keyserver.cais.rnp.br:11371/` utilizando o ID (`0x5B1B5A3BD6CEE72D`). Em seguida, foi gerado um certificado de revogação, importado e enviado ao servidor de chaves da RNP:

```
$ gpg -o revokee.asc --gen-revoke --armor 5B1B5A3BD6CEE72D
$ gpg --import revokee.asc
$ gpg --keyserver keyserver.cais.rnp.br --send-keys 5B1B5A3BD6CEE72D
```

Depois de feitos todos esses passos, ao se tentar ver sobre as chaves guardadas localmente, é possível ver que a revogação foi satisfeita:

```
$ gpg --list-secret-keys --keyid-format LONG
/home/jptiz/.gnupg/pubring.kbx
------------------------------
sec   rsa2048/C598C13DF4964793 2019-04-26 [SC]
      48F1744C8CCB4C04A7A6F2B9C598C13DF4964793
uid                 [ultimate] João Paulo Taylor Ienczak Zanette (For educational
↪  purposes) <jpaulotiz@gmail.com>
ssb   rsa2048/B11690E2A8DDA995 2019-04-26 [E]

sec   rsa2048/5B1B5A3BD6CEE72D 2019-04-26 [SC] [revoked: 2019-04-26]
      F6055CCED33CE15CC2A8065A5B1B5A3BD6CEE72D
uid                 [ revoked] João Paulo Taylor Ienczak Zanette (More educational
↪  purpooooooses) <jpaulotiz@gmail.com>

sec   rsa2048/1DFE185BDCAE898A 2019-04-29 [SC]
      BC50CCDA2D2DBAD0302EFEAD1DFE185BDCAE898A
uid                 [ultimate] João Paulo Taylor Ienczak Zanette (Forgot last password :P
↪  For studying purposes.) <jpaulotiz@gmail.com>
ssb   rsa2048/79D4F9460C7144E8 2019-04-29 [E]
```

Também é possível ver a confirmação acessando `http://keyserver.cais.rnp.br:11371/` (Figura 1).

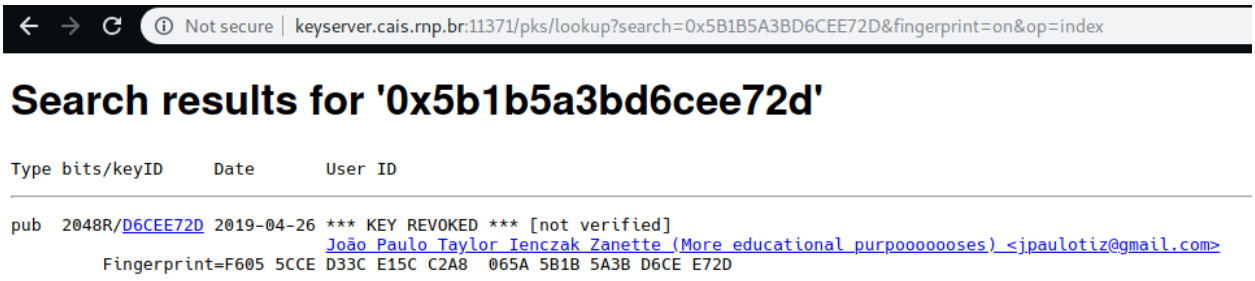

Figura 1: Confirmação da revogação do certificado `5B1B5A3BD6CEE72D`.

Parte 3. Assinatura e Revogação de Assinatura

3. Pratique a revogação de assinaturas e certificados GPG. Assine um certificado qualquer GPG (de outra pessoa). E envie esse certificado para o servidor GPG. Depois verifique o status do certificado. E então, revogue a assinatura que você fez. Confira o resultado no servidor GPG.

   ☐ Faça um relatório do que você fez, incluindo o KeyID do certificado cuja assinatura você revogou.

1. Foi importada a chave de “Adriano Tosetto” pelo servidor do RNP (salva em um arquivo .asc e então importada com `gpg --import <arquivo>.asc`);

2. Em seguida, foram executados os comandos para assinar e gerar um arquivo de assinatura:

```
$ gpg --local-user 1DFE185BDCAE898A --sign-key adriano.rafael10@hotmail.com
$ gpg --output ~/tosetto-signed.key --export --armor adriano.rafael10@hotmail.com
```

3. O conteúdo do arquivo `tosetto-signed.key` foi enviado ao servidor da RNP como uma chave, confirmando a assinatura (Figura 2);

4. A assinatura foi revogada localmente utilizando:

```
$ gpg --edit-key 52A4FF6D1F0CC9B8 # Editar a chave
gpg> revsig
Your decision? 0
Enter an optional description; end it with an empty line:
> My teacher asked. Sorry :(
>
Is this okay? (y/N) y
gpg> Save changes? (y/N) y
$ gpg --keyserver keyserver.cais.rnp.br --send-key 52A4FF6D1F0CC9B8 \
    # Enviar chave ao servidor da RNP
gpg: sending key 52A4FF6D1F0CC9B8 to hkp://keyserver.cais.rnp.br
$ gpg --keyserver keyserver.cais.rnp.br --recv-key 52A4FF6D1F0CC9B8 \
    # Atualizar dados da chave
```

5. Após isso, é acessando o site é possível ver que a assinatura foi revogado (Figura 3).

```
uid Adriano Tosetto <adriano.rafael10@hotmail.com>
sig  sig3  1F0CC9B8 2019-04-27 __________ 2021-04-26 [selfsig]
sig  sig   0F7EFC5D 2019-04-27 __________ __________ Gustavo Olegario <gustavo-olegario@hotmail.com>
sig  sig   779F2B26 2019-04-29 __________ __________ Theo Regis (Graduando de CCO - UFSC) <theo.regis@grad.ufsc.br>
sig  sig   DCAE898A 2019-04-30 __________ __________ João Paulo Taylor Ienczak Zanette (Forgot last password :P For studying purposes.) <jpaulotiz@gmail.com>

uat [contents omitted]
sig  sig3  1F0CC9B8 2019-04-30 __________ 2021-04-26 [selfsig]

sub  3072R/FC46CC8F 2019-04-27
sig sbind  1F0CC9B8 2019-04-27 __________ 2021-04-26 []
```

Figura 2: Certificado de Adriano Tosetto assinado.

```
uid Adriano Tosetto <adriano.rafael10@hotmail.com>
sig  sig3  1F0CC9B8 2019-04-27 __________ 2021-04-26 [selfsig]
sig  sig   0F7EFC5D 2019-04-27 __________ __________ Gustavo Olegario <gustavo-olegario@hotmail.com>
sig  sig   779F2B26 2019-04-29 __________ __________ Theo Regis (Graduando de CCO - UFSC) <theo.regis@grad.ufsc.br>
sig revok  DCAE898A 2019-04-30 __________ __________ João Paulo Taylor Ienczak Zanette (Forgot last password :P For studying purposes.) <jpaulotiz@gmail.com>
```

Figura 3: Certificado de Adriano Tosetto com assinatura revogada.

Parte 4. Anel de Chaves (Keyring)

> 4. O que é o anel de chaves privadas? Como este está estruturado? Na sua aplicação GPG onde este anel de chaves é armazenado? Quem pode ser acesso a esse porta chaves?

O anel de chaves é quem organiza as chaves guardadas em um servidor (local ou remoto), funcionando como um chaveiro. Esse anel é armazenado como uma lista sequencial de chaves em um arquivo, em que cada chave contém:

Carimbo de tempo: quando o par foi gerado;

ID da chave: 64 bits mais significativos da chave pública;

Chave pública: a parte pública da chave;

Chave privada: a parte privada da chave, criptografada com uma senha;

ID do usuário: geralmente o e-mail do usuário.

O chaveiro padrão fica localizado na pasta `${HOME}/.gnupg`. Qualquer um possui acesso ao chaveiro, porém apenas quem tiver a senha pode ter acesso à chave privada.

Parte 5. Sobre assinatura local e remota

> 5. Qual a diferença entre assinar uma chave local e assinar no servidor?

A disponibilidade da assinatura: uma chave local possui assinatura conhecida apenas localmente, enquanto em um servidor há, geralmente, uma replicação da assinatura em outros servidores.

Parte 6. Banco de dados de confiabilidade

> 6. O que é e como é organizado o banco de dados de confiabilidade?

O banco de dados de confiabilidade é simplesmente um arquivo (.db) que contém uma lista de quais chaves o usuário dono do chaveiro possui confiança.

Parte 7. Sub-chaves

> 7. O que são e para que servem as sub-chaves?

São como chaves normais, porém ligadas a um par de chaves mestre. Servem tanto para assinatura quanto criptografia, com a vantagem de poderem ser revogadas independentemente da chave mestre e sendo guardadas separadamente.

Parte 8. Representação própria em um certificado

> 8. Coloque sua foto (ou uma figura qualquer) que represente você em seu certificado GPG.

OK.

Parte 9. Servidor de chaves

> 9. O que é preciso para criar e manter um servidor de chaves GPG, sincronizado com os demais servidores existentes?

É preciso utilizar o protocolo SKS. Para sincronizar automaticamente em um servidor, pode-se criar um processo *daemon*, configurar quais os outros servidores SKS, fazer o download dos arquivos de banco de dados (e importá-los) deles, configurar o servidor web (com NGinx, por exemplo) que irá fazer a sincronização e então iniciar o *daemon*.

Parte 10. Arquivos sigilosos

> 10. Dê um exemplo de como tornar sigiloso um arquivo usando o GPG. Envie esse arquivo para um colega e que enviar para você outro arquivo cifrado. Você deve decifrar e recuperar o conteúdo original.

Basta criptografar o arquivo utilizando alguma chave pública válida do destinatário. Ao mandar um arquivo criptografado para o Adriano Tosetto, foi possível que ele descriptografasse o arquivo com uma chave dele e obtivesse o conteúdo original.

Parte 11. Assinatura de arquivos

> 11. Mostre um exemplo de como assinar um arquivo (assinatura anexada e outro com assinatura separada), usando o GPG. Envie uma mensagem assinada para um colega. Esse colega deve enviar para você outra mensagem assinada. Verifique se a assinatura está correta.

Um arquivo de texto foi enviado a Adriano Tosetto, decriptografado e com a resposta recebida corretamente (Figura 4).

Figura 4: Arquivo decriptografado.