Segurança em Computação
Trabalho Individual III

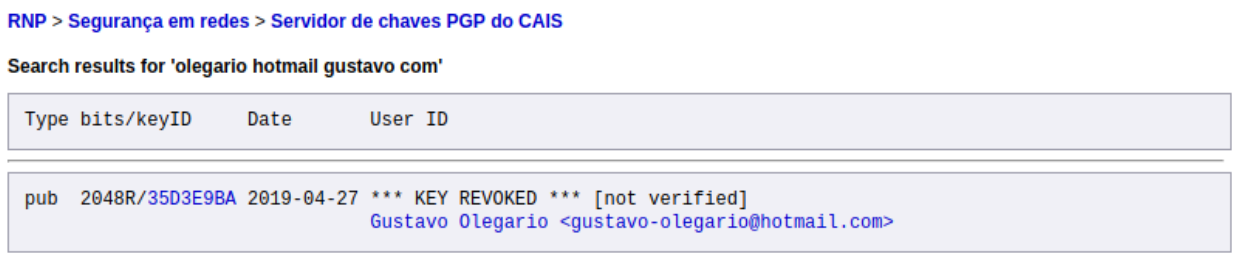
Gustavo Figueira Olegário

30 de abril de 2019

1 Primeira parte do relatório

KEYID: B6796D2435D3E9BA
Para cumprir a primeira parte do trabalho, criou-se um par de chave pública/privada. Para criar esse par de chaves, seguiu-se o tutorial disponibilizado no seguinte link. As secções utilizadas desse guia foram: `Generating an OpenPGP Key`, `Setting the key to be the default`, `Adding Encryption Capabilities`, `Creating a revocation certificate`, `Making an ASCII armored version of your public key`.

Após seguir os passos descritos nesse tutorial, acessou-se o seguinte site da RNP: https://memoria.rnp.br/keyserver.php. Com o conteúdo do arquivo `mykey.asc` copiado, colou-se o mesmo na caixa de conteúdo da secção *Submissão de chaves* e clicou-se no botão enviar. Fez-se, em seguida, uma busca por chave através do email para garantir de que a chave havia sido cadastrada. Por último, seguiu-se os comandos da secção `Não tenho o certificado de revogação`, no próprio site da RNP, para revogar a chave enviada. Para garantir que o processo havia sido executado com sucesso, procurou-se novamente a chave através do email gerador (i.e. `gustavo-olegario@hotmail.com`) e pode ser constatado, como mostra o *print* abaixo, que tudo havia ocorrido como esperado.

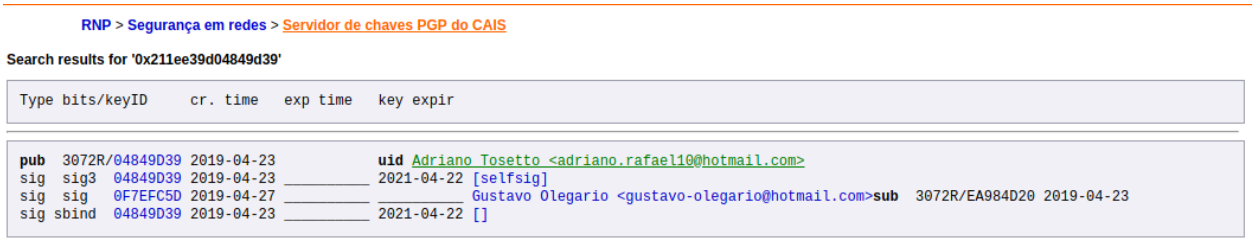


2 Primeira parte do relatório

Para essa segunda parte do relatório, assinou-se a chave pública com o seguinte ID: 04849D39. Inicialmente, criou-se um novo par de chave público e privada, já que a última foi revogada, seguindo os mesmos passos do item anterior. Após isso, encontrou-se uma chave pública qualquer do repositório da RNP, nesse caso do indivíduo: `adriano.rafael10@hotmail.com`. Em seguida utilizou-se os seguintes comandos para assinar e reenviar a chave para o servidor:

```
$ gpg --recv-keys 04849D39
$ gpg --sign-key 04849D39
$ gpg --keyserver keyserver.cais.rnp.br --send-keys 04849D39
```

Em seguida, ao buscar a chave novamente no site da RNP, é possível notar pelo *print* abaixo que a operação foi realizada com sucesso.



Para revogar a assinatura da chave, execoute-se a seguinte lista de comandos:

```
gpg --edit-key 04849D39
gpg> revsig
Really create the revocation certificates? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  4 = User ID is no longer valid
  Q = Cancel
Your decision? 0
Enter an optional description; end it with an empty line:
>
Reason for revocation: No reason specified
(No description given)
Is this okay? (y/N) y
gpg> save
```

Por último, abriu-se novamente o repositório e pode-se certificar que a revogação da assinatura da chave havia sido executada.

3 Questionário

Questão 4: um anel de chaves é um arquivo que contém um conjunto de chaves que podem ser dividas entre mestre e sub-chaves. As sub-chaves são utilizadas para encriptar as mensagens e realizar assinaturas, enquanto que a chave mestra é usada para identificar nome e usuário do dono do certificado. Além disso, ela é também utilizada para assinar as subchaves, para provar que elas realmente existem no certificado. Esse arquivo pode ser encontrado no seguinte caminho: `~/.gnupg/pubring.kbx`. Por guardar somente chaves públicas, não há necessidade de restringir as pessoas que podem ter acesso a esse arquivo.

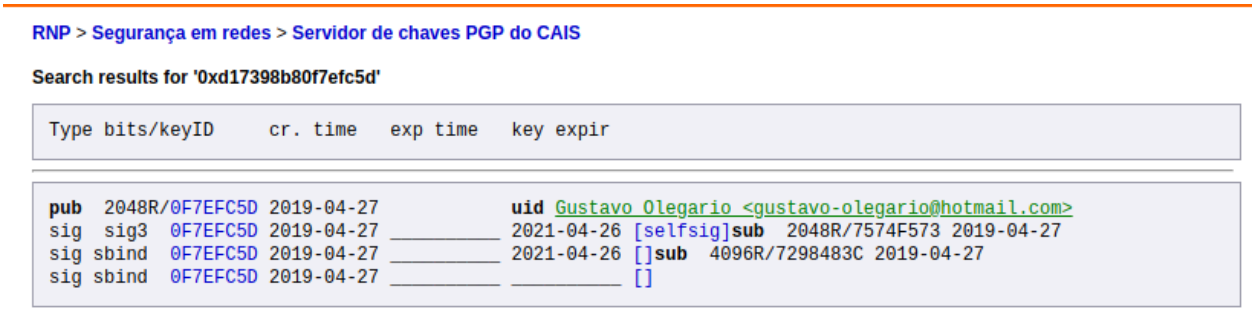
Questão 5: a diferença é que ao assinar a chave localmente, para a assinatura ser detectada por outros usuários, ela precisa ser publicada no servidor. Enquanto que, ao assinar a chave diretamente no servidor, a assinatura já fica automática exposta a todos.

Questão 6: TODO

Questão 7: As sub-chaves são chaves públicas integrantes do arquivo de anel de chaves. Elas são utilizadas

para encriptar as mensagens e realizar assinaturas.

Questão 8:



Questão 9: É preciso utilizar algum sistema de banco distribuído, baseado em um algoritmo de *2 Phase Commit* em que um nodo mestre antes de alterar uma chave, deve avisar os nodos de sua rede que uma alteração será feita, estes por sua vez respondem com um *Prepare* a mensagem recebida. Então o nodo mestre altera a chave, e os nodos filhos são informados fazendo a alteração da informação.

Questão 10: Para realizar essa tarefa, basta que um colega baixe a minha chave pública de um repositório de chaves públicas, cifre a mensagem com a chave, me envie o arquivo e ao receber esse arquivo eu decifre a mensagem utilizando minha chave privada. Para isso basta que o meu colega execute o seguintes comandos:

```
$ gpg --keyserver keyserver.cais.rnp.br --output encrypted.gpg --encrypt --recipient
    gustavo-olegario@hotmail.com decrypted.txt
```

De posse do arquivo, basta que eu execute:

```
$ gpg --output decrypted.txt --decrypt encrypted.gpg
```

Questão 11: Para criar um arquivo assinado digitalmente usando GPG, com assinatura anexada, basta executar o seguinte comando:

```
$ gpg --output decrypted.sig --sign decrypted.txt
```

Para verificar a assinatura basta executar:

```
$ gpg --output decrypted.txt --decrypt decrypted.sig
gpg: Signature made Sat 27 Apr 2019 19:02:04 -03
gpg:              using RSA key 1B60394F6B1938D4350069CCD17398B80F7EFC5D
gpg: Good signature from "Gustavo Olegario <gustavo-olegario@hotmail.com>" [ultimate]
```

Para gerar um arquivo com assinatura separada basta utilizar:

```
$  gpg --output decrypted.sig --detach-sign decrypted.txt
```

E para conferir a assinatura basta executar:

```
$  gpg --verify decrypted.sig decrypted.txt
```

Ao receber um arquivo assinado pelo meu colega, além do arquivo, é necessário possuir seu KEYID. Assim, executa-se o seguintes comandos:

```
$ gpg --recv-key 1F0CC9B8
$ gpg --verify decrypted.sig
```