Usando o GPG para Autenticação e Criptografia

O **GPG** (GNU pgp, versão livre da ferramenta pgp) permite encriptar dados, assim somente o destinatário terá acesso aos dados, adicionalmente poderá verificar se a origem dos dados é confiável (através da assinatura de arquivos). O sistema PGP se baseia no conceito de chave *pública* e *privada*: Sua chave *pública* é distribuída para as pessoas que deseja trocar dados/mensagens e a chave *privada* fica em sua máquina (ela não pode ser distribuída). As chaves públicas e privadas são armazenadas nos arquivos `pubring.gpg` e `secring.gpg` respectivamente, dentro do subdiretório `~/.gnupg`. Veja "Criando um par de chaves pública/privada" para criar este par de chaves.

Os dados que recebe de outra pessoa são criptografados usando sua chave pública e somente você (de posse da chave privada) poderá desencriptar os dados. Quando assina um arquivo usando o pgp, ele faz isto usando sua chave privada, o destinatário de posse da chave pública poderá então confirmar que a origem dos dados é confiável.

O **gpg** vem largamente sendo usado para transmissão segura de dados via internet. Muitos programas de e-mails como o **mutt** e **sylpheed** incluem o suporte a pgp embutido para envio de mensagens assinadas/encriptadas (MIME não tem uma codificação segura e não garante que a mensagem vem de quem realmente diz ser). Um servidor de e-mail no **Linux** configurado como as mesmas configurações/endereços do provedor da vítima pode enganar com sucesso um usuário passando-se por outro.

Instalando o PGP

apt-get install gnupg

Após instalar o , execute o comando **gpg** para criar o diretório `~/.gnupg` que armazenará as chaves pública e privada.

Criando um par de chaves pública/privada

Para gerar um par de chaves pessoais use o comando `gpg --gen-key`. Ele executará os seguintes passos:

1. `Chave criptográfica` - Selecione *DSA e ELGamal* a não ser que tenha necessidades específicas.
2. `Tamanho da chave` - 1024 bits traz uma boa combinação de proteção/velocidade.
3. `Validade da chave` - 0 a chave não expira. Um número positivo tem o valor de dias, que pode ser seguido das letras `w` (semanas), `m` (meses) ou `y` (anos). Por exemplo, "7m", "2y", "60".

   Após a validade, a chave será considerada inválida.
4. `Nome de usuário` - Nome para identificar a chave
5. `E-mail` - E-mail do dono da chave
6. `comentário` - Uma descrição sobre a chave do usuário.
7. `Confirmação` - Tecle "O" para confirmar os dados ou uma das outras letras para modificar os dados de sua chave.
8. `Digite a FraseSenha` - Senha que irá identificá-lo(a) como proprietário da chave privada. É chamada de FraseSenha pois pode conter espaços e não há limite de caracteres. Para alterá-la posteriormente,

siga as instruções em "Mudando sua FraseSenha".

9. `Confirme e aguarde a geração da chave pública/privada.`

Encriptando Dados

Use o comando `gpg -e arquivo` faz a encriptação de dados:

```
gpg -e arquivo.txt
```

Será pedida a identificação de usuário, digite o nome que usou para criar a chave. O arquivo criado será encriptado usando a chave pública do usuário (`~/.gnupg/pubring.gpg`) e terá a extensão `.gpg` adicionada (`arquivo.txt.gpg`). Além de criptografado, este arquivo é compactado (recomendável para grande quantidade de textos). A opção *-a* é usada para criar um arquivo criptografado com saída ASCII 7 bits:

```
gpg -e -a arquivo.txt
```

O arquivo gerado terá a extensão `.asc` acrescentada (`arquivo.txt.asc`) e não será compactado. A opção *-a* é muito usada para o envio de e-mails.

Para criptografar o arquivo para ser enviado a outro usuário, você deverá ter a chave pública do usuário cadastrado no seu chaveiro (veja "Adicionando chaves públicas ao seu chaveiro pessoal") e especificar a opção *-r* seguida do nome/e-mail/ID da chave pública:

```
gpg -r kov -e arquivo.txt
```

O exemplo acima utiliza a chave pública de kov para encriptar o arquivo `arquivo.txt` (somente ele poderá decriptar a mensagem usando sua chave privada).

OBS: É recomendável especificar o nome de arquivo sempre como último argumento.

Decriptando dados com o GPG

Agora vamos fazer a operação reversa da acima, a opção *-d* é usada para decriptar os dados usando a chave privada:

```
gpg -d arquivo.txt.asc >arquivo.txt
gpg -d arquivo.txt.gpg >arquivo.txt
```

Descriptografa os arquivos `arquivo.txt.asc` e `arquivo.txt.gpg` recuperando seu conteúdo original. A sua "FraseSenha" será pedida para descriptografar os dados usando a chave privada (`~/.gnupg/secring.gpg`).

Assinando arquivos

Assinar um arquivo é garantir que você é a pessoa que realmente enviou aquele arquivo. Use a opção *-s* para assinar arquivos usando sua chave privada:

```
gpg -s arquivo.txt
```

A "FraseSenha" será pedida para assinar os dados usando sua chave privada. Será gerado um arquivo `arquivo.txt.gpg` (assinado e compactado). Adicionalmente a opção *--clearsign* poderá ser usada para fazer uma assinatura em um texto plano, este é um recurso muito usado por programas de e-mails com suporte ao gpg:

```
gpg -s --clearsign arquivo.txt
```

Será criado um arquivo chamado `arquivo.txt.asc` contendo o arquivo assinado e sem compactação.

Checando assinaturas

A checagem de assinatura consiste em verificar que quem nos enviou o arquivo é realmente quem diz ser e se os dados foram de alguma forma alterados. Você deverá ter a chave pública do usuário no seu chaveiro para fazer esta checagem (veja "Adicionando chaves públicas ao seu chaveiro pessoal"). Para verificar os dados assinados acima usamos a opção *--verify*:

```
gpg --verify arquivo.txt.asc
```

Se a saída for "Assinatura Correta", significa que a origem do arquivo é segura e que ele não foi de qualquer forma modificado.

```
gpg --verify arquivo.txt.gpg
```

Se a saída for "Assinatura INCORRETA" significa que ou o usuário que enviou o arquivo não confere ou o arquivo enviado foi de alguma forma modificado.

Extraindo sua chave pública do chaveiro

Sua chave pública deve ser distribuída a outros usuários para que possam enviar dados criptografados ou checar a autenticidade de seus arquivos. Para exportar sua chave pública em um arquivo que será distribuído a outras pessoas ou servidores de chaves na Internet, use a opção *--export*:

```
gpg --export -a usuario >chave-pub.txt
```

Ao invés do nome do usuário, poderá ser usado seu e-mail, ID da chave, etc. A opção *-a* permite que os dados sejam gerados usando bits ASCII 7.

Adicionando chaves públicas ao seu chaveiro pessoal

Isto é necessário para o envio de dados criptografados e checagem de assinatura do usuário, use a opção *--import*:

```
gpg --import chave-pub-usuario.txt
```

Assumindo que o arquivo `chave-pub-usuario.txt` contém a chave pública do usuário criada em "Extraindo sua chave pública do chaveiro". O **gpg** detecta chaves públicas dentro de textos e faz a extração corretamente. Minha chave pública pode ser encontrada em "Chave Pública PGP" ou http://pgp.ai.mit.edu.

Listando chaves de seu chaveiro

Use o comando `gpg --list-keys` para listar as chaves pública do seu chaveiro. O comando `gpg --list-secret-keys` lista suas chaves privadas.

Apagando chaves de seu chaveiro

Quando uma chave pública é modificada ou por qualquer outro motivo deseja retira-la do seu chaveiro público, utilize a opção *--delete-key*:

```
gpg --delete-key usuario
```

Pode ser especificado o nome de usuário, e-mail IDchave ou qualquer outro detalhe que confira com a chave pública do usuário. Será pedida a confirmação para excluir a chave pública.

OBS: A chave privada pode ser excluída com a opção *--delete-secret-key*. Utilize-a com o máximo de atenção para excluir chaves secretas que não utiliza (caso use mais de uma), a exclusão acidental de sua chave secreta significa é como perder a chave de um cofre de banco: você não poderá descriptografar os arquivos enviados a você e não poderá enviar arquivos assinados.

Mesmo assim se isto acontecer acidentalmente, você poderá recuperar o último backup da chave privada em `~/.gnupg/secring.gpg~`.

Mudando sua FraseSenha

Execute o comando `gpg --edit-key usuário`, quando o programa entrar em modo de comandos, digite `passwd`. Será lhe pedida a "Frase Senha" atual e a nova "Frase Senha". Digite "save" para sair e salvar as alterações ou "quit" para sair e abandonar o que foi feito.

O `gpg --edit-key` permite gerenciar diversos aspectos de suas chaves é interessante explora-lo digitando "?" para exibir todas as opções disponíveis.

Assinando uma chave digital

A assinatura de chaves é um meio de criar laços de confiança entre usuários PGP. Assinar uma chave de alguém é algo sério, você deve ter noção do que isto significa e das conseqüências que isto pode trazer antes de sair assinando chaves de qualquer um.

O próprio teste para desenvolvedor da distribuição **Debian** requer como primeiro passo a identificação do candidato, caso sua chave pgp seja assinada por algum desenvolvedor desta distribuição, imediatamente o teste de identificação é completado. A partir disso você deve ter uma noção básica do que isto significa. Para assinar uma chave siga os seguintes passos:

1. Importe a chave pública do usuário (veja “Adicionando chaves públicas ao seu chaveiro pessoal”).

2. Execute o comando `gpg --edit-key usuario` (onde *usuario* é o nome do usuário/e-mail/IDchave da chave pública importada).

3. Digite `list`, e selecione a chave pública (pub) do usuário com o comando `uid [numero_chave]`. Para assinar todas as chaves públicas do usuário, não selecione qualquer chave com o comando `uid`.

4. Para assinar a chave pública do usuário digite `sign`, será perguntado se deseja realmente assinar a chave do usuário e então pedida a "FraseSenha" de sua chave privada.

5. Digite "list", repare que existe um campo chamado `trust: n/q` no lado direito. O primeiro parâmetro do "trust" indica o valor de confiança do dono e o segundo (após a `/`) o valor de confiança calculado automaticamente na chave. As seguintes possuem o seguinte significado:

   - `-` - Nenhum dono encontrado/confiança não calculada.
   - `e` - Chave expirada/falha na checagem de confiança.
   - `q` - Quando não conhece o usuário.
   - `n` - Quando não confia no usuário (é o padrão).
   - `m` - Pouca confiança no usuário.
   - `f` - Totalmente confiável.
   - `u` - Indiscutivelmente confiável. Somente usado para especificar a chave pública do próprio usuário.

   O valor de confiança da chave pode ser modificado com o comando `trust` e selecionando uma das opções de confiança. Os valores de confiança para a chave pública pessoal é `-/u` (não é necessário calcular a confiança/indiscutivelmente confiável).

Listando assinaturas digitais

Execute o comando `gpg --list-sigs` para listas todas as assinaturas existentes no seu chaveiro. Opcionalmente pode ser especificado um parâmetro para fazer referência a assinatura de um usuário:`gpg --list-sigs usuario`.

O comando `gpg --check-sigs` adicionalmente faz a checagem de assinaturas.

Recomendações para a assinatura de chaves GPG

Este texto foi divulgado publicamente em 22 de Maio de 2001 por `Henrique de Moraes Holschuh` na lista <debian-user-portuguese@lists.debian.org> explicando os procedimentos de segurança para a troca de chaves públicas individuais e em grupo de usuários. Ele é um pouco longo mas a pessoa é especializada no assunto, e seu foco é a segurança na troca de chaves e o que isto significa. Após consulta ao autor do texto, o texto foi reproduzido na íntegra, mantendo os padrões de formatação da mensagem.

```
Trocando assinaturas de chaves digitais

Direitos de republicação cedidos ao domínio público, contanto que o texto
seja reproduzido em sua íntegra, sem modificações de quaisquer espécie, e
incluindo o título e nome do autor.


1. Assinaturas digitais
2. Chaves digitais e a teia de confiança
3. Trocando assinaturas de chaves digitais com um grupo de pessoas


1. Assinaturas digitais

Uma assinatura digital é um número de tamanho razoável (costuma ter de 128 a
160 bits) que representa um bloco bem maior de informação, como um e-mail.

Pense numa assinatura como se ela fosse uma versão super-comprimida de um
texto.  Se você muda alguma coisa (por menor que seja) no texto que uma
assinatura "assina", essa assinatura se torna inválida: ela não mais
representa aquele texto.

Existe uma relação direta entre uma assinatura e informação que ela assina.
Se uma das duas for modificada, elas passam a não mais "combinar" uma com a
a outra. Um programa de computador pode detectar isso, e avisar que a
assinatura é "inválida".

Os algoritmos mais usados para criar e verificar assinaturas digitais são o
SHA-1, RIPEM160 e MD5.  O MD5 não é considerado tão bom quanto os outros
dois.

Assinaturas digitais também funcionam com arquivos "binários", ou seja:
imagens, som, planilhas de cálculo... e chaves digitais.


2. Chaves digitais e a teia de confiança

Chaves digitais são fáceis de falsificar, você só precisa criar uma chave
nova no nome de sicrano, por um endereço de e-mail novinho em folha daqueles
que você consegue nesses webmail da vida, e pronto.  Agora é só espalhar
essa chave por aí que os bestas vão usá-la pensando que é de sicrano.

A menos que os "bestas" não sejam tão bestas assim, tenham lido o manual do
seu software de criptografia, e saibam usar assinaturas e a teia de
confiança para verificar se a tal chave é de sicrano mesmo.

Programas de criptografia (os bons, tipo PGP e GNUpg) usam um sistema de
assinaturas nas chaves digitais para detectar e impedir esse tipo de
problema:  Ao usuário é dado o poder de "assinar" uma chave digital, dizendo
"sim, eu tenho certeza que essa chave é de fulano, e que o e-mail de fulano é
esse que está na chave".

Note bem as palavras "certeza", e "e-mail".  Ao assinar uma chave digital,
você está empenhando sua palavra de honra que o _nome_ do dono de verdade
daquela chave é o nome _que está na chave_, e que o endereço de e-mail
daquela chave é da pessoa (o "nome") que também está na chave.
```

Se todo mundo fizer isso direitinho (ou seja, não sair assinando a chave de qualquer um, só porque a outra pessoa pediu por e-mail, ou numa sala de chat), cria-se a chamada teia de confiança.

Numa teia de confiança, você confia na palavra de honra dos outros para tentar verificar se uma chave digital é legítima, ou se é uma "pega-bobo".

Suponha que Marcelo tenha assinado a chave de Cláudia, e que Roberto, que conhece Marcelo pessoalmente e assinou a chave de Marcelo, queira falar com Cláudia.

Roberto sabe que Marcelo leu o manual do programa de criptografia, e que ele não é irresponsável. Assim, ele pode confiar na palavra de honra de Marcelo que aquela chave digital da Cláudia é da Cláudia mesmo, e usar a chave pra combinar um encontro com Cláudia.

Por outro lado, Roberto não conhece Cláudia (ainda), e não sabe que tipo de pessoa ela é. Assim, rapaz prevenido, ele não confia que Cláudia seja uma pessoa responsável que verifica direitinho antes de assinar chaves.

Note que Roberto só confiou na assinatura de Marcelo porque, como ele já tinha assinado a chave de Marcelo, ele sabe que foi Marcelo mesmo quem assinou a chave de Cláudia.

Enrolado? Sim, é um pouco complicado, mas desenhe num papel as flechinhas de quem confia em quem, que você entende rapidinho como funciona.

O uso da assinatura feita por alguém cuja chave você assinou, para validar a chave digital de um terceiro, é um exemplo de uma pequena teia de confiança.

3. Trocando assinaturas de chaves digitais com um grupo de pessoas

Lembre-se: ao assinar uma chave digital, você está empenhando sua palavra de honra que toda a informação que você assinou naquela chave é verdadeira até onde você pode verificar, _e_ que você tentou verificar direitinho.

Pense nisso como um juramento: "Eu juro, em nome da minha reputação profissional e pessoal, que o nome e endereços de e-mail nessa chave são realmente verdadeiros até onde posso verificar, e que fiz uma tentativa real e razoável de verificar essa informação."

Sim, é sério desse jeito mesmo. Você pode ficar muito "queimado" em certos círculos se você assinar uma chave falsa, pensando que é verdadeira: a sua assinatura mal-verificada pode vir a prejudicar outros que confiaram em você.

Bom, já que o assunto é sério, como juntar um grupo de pessoas numa sala, e trocar assinaturas de chaves entre si? Particularmente se são pessoas que você nunca viu antes? Siga o protocolo abaixo, passo a passo, e sem pular ou violar nenhum dos passos.

1 - Reúna todos em uma sala, ou outro local não tumultuado, pressa e bagunça são inimigas da segurança.

2 - Cada um dos presentes deve, então, ir de um em um e:

    2.1 - Apresentar-se, mostrando _calmamente_ documentação original (nada de fotocópia) comprovando sua identidade. RG, CPF, passaporte, certidão de nascimento ou casamento, carteira de motorista, cartão de crédito são todos bons exemplos. Só o RG sozinho não é -- tem muito RG falsificado por aí -- mas o RG junto com o cartão de banco já seria suficiente. Se nenhum documento tiver foto, também não é o bastante.

        * Se alguém pedir o documento na mão, para verificar direitinho, não leve pro lado pessoal. Deixe a pessoa

```
            verificar até estar satisfeita (mas não descuide do
            documento). Isso só significa que ela leva muito a sério a
            responsabilidade de assinar chaves.

      2.2 -  Entregar um papel com as informações da chave: Nome
            (QUE OBRIGATORIAMENTE PRECISA SER O MESMO NOME CONSTANTE NOS
            DOCUMENTOS APRESENTADOS EM 2.1), e-mail, número da chave
            (keyID), e fingerprint da chave (assinatura digital da chave)

            RECIPIENTE DO PAPEL: Se você achar que os documentos que te
            apresentaram não são prova suficiente, talvez porque o nome
            não bate com o da chave, ou porque uma foto nos documentos não
            está parecida com quem mostrou os documentos, marque
            discretamente no papel, porque você NÃO deve assinar essa
            chave.   Se achar que o outro vai engrossar, não diga para ele
            que não vai assinar a chave dele.

  3 -  Pronto. Podem ir embora, porque o resto dos passos deve ser feito com
       calma, em casa.  Lembre-se que você não vai estar efetuando nenhum
       julgamento moral a respeito de quem você assinar a chave. Você só irá
       afirmar que a chave de sicrano é realmente aquela, e mais nada.

  4 -  Para cada uma das chaves que você marcou no papel que "posso assinar":

      4.1 -  Peça para o seu programa de criptografia mostrar a chave e sua
            assinatura (fingerprint).

            SE: O nome no papel for exatamente igual ao nome na chave
            (user ID/UID da chave). E: A assinatura no papel for
            exatamente igual à assinatura na chave (fingerprint).  ENTÃO:
            Vá para o passo 4.3.

      4.2 -  As informações não bateram, por isso você não deve assinar a
            chave.  Se quiser, envie um e-mail avisando que não poderá
            assinar a chave. Não aceite tentativas de retificação por
            e-mail ou telefone. Um outro encontro face-à-face, refazendo
            todos os passos 2.1 e 2.2 é o único jeito de retificar
            o problema.

      4.3 -  As informações bateram, o que garante que o *nome* está
            correto. Agora é preciso ter certeza do endereço de e-mail.
            Para isso, envie uma e-mail *CIFRADA* pela chave que você está
            testando, para o endereço de e-mail constante na chave.  Nessa
            e-mail, coloque uma palavra secreta qualquer e peça para o
            destinatário te responder dizendo qual a palavra secreta que
            você escreveu. Use uma palavra diferente para cada chave que
            estiver testando, e anote no papel daquela chave qual palavra
            você usou.

      4.4 -  Se você receber a resposta contendo a palavra secreta correta,
            você pode assinar a chave. Caso contrário, não assine a chave --
            o endereço de e-mail pode ser falso.


Comandos do gpg (GNUpg) correspondentes a cada passo:
  2.2 -       gpg --fingerprint <seu nome ou 0xSuaKEYID>
              (retorna as informações que devem estar no papel a ser
              entregue no passo 2.2)

  4.1 -       gpg --receive-key <0xKEYID>
              (procura a chave especificada nos keyservers)
              gpg --sign-key <0xKEYID>
              (assina uma chave)

              Assume-se que você sabe cifrar e decifrar mensagens. Caso
              não saiba, ainda não é hora de querer sair assinando chaves.
```

Anterior
Alternativas seguras a serviços sem criptografia

Subir
Voltar ao Índice

Próximo
Criptografia de blocos usando DM-Crypt / cryptsetup