Universidade da Beira Interior
Faculdade de Engenharia
Departamento de Informática

Segurança Informática
Guia para Aula Laboratorial 9
Licenciatura em Engenharia Informática
Licenciatura em Informática Web
Licenciatura em Tecnologias e Sistemas da Informação

Computer Security
Guide for Laboratory Class 9
Degree in Computer Science and Engineering
Degree in Web Informatics
Degree in Information Technologies and Systems

Sumário
Aula laboratorial dedicada à utilização de uma aplicação *Pretty Good Privacy* (PGP) (*Gnu Privacy Guard* – GPG). Abordam-se temas como a criação de um par de chaves assimétricas referente ao titular, importação de chaves de outros utilizadores do PGP, utilização do serviço de confidencialidade (cifra), autenticação (assinatura digital) e configuração da tabela de confiança.

Summary
Laboratory practice dedicated to the utilization of a Pretty Good Privacy (PGP) application (Gnu Privacy Guard – GPG). This class addresses topics concerning the generation of asymmetric keys for the user, importing keys to the public keyring, using the confidentiality (encryption) and autentication (digital signatures) services, and configuration of the trust table.

Pré-requisitos:
Algumas das tarefas propostas a seguir requerem o acesso a um sistema que disponibilize a ferramenta *GNU Privacy Guard* (GPG). Sugere-se, assim, o uso de uma distribuição comum de Linux, onde esta condição estará provavelmente preenchida à partida.

1 Criação de Pares de Chaves Assimétricas

Creation of Asymmetric Key Pairs

O objetivo principal desta aula prática é aprender a lidar com o PGP através da ferramenta GPG. [1] O passo inicial obrigatório para quem quer utilizar o PGP consiste na geração de um par de chaves assimétricas (possivelmente RSA).

Q1.: O que significa GPG?

G _____ P _____ G _____

Q2.: O que significa RSA?

R _____ S _____ A _____

[1] Mais informação acerca desta ferramenta pode ser encontrada em http://www.gnupg.org/.

Tarefa 1 ***Task 1***

No seu sistema com uma instalação do GPG, abra uma consola/terminal e escreva o seguinte comando:

```
$ gpg --help
```

Q3.: Qual é a versão do GPG que está a utilizar?

É a versão _____

Tarefa 2 ***Task 2***

Q4.: Qual dos seguintes comandos gera pares de chaves para o utilizador do GPG?

- ☐ `$ gpg --new-keys`
- ☐ `$ gpg --new`
- ☐ `$ gpg --gen-key`
- ☐ `$ oh-gpg-gera-lá!-se-faz-favor`

Depois de descobrir qual o comando certo para gerar pares de chaves, emita-o no terminal e certifique-se que os seguintes requisitos são preenchidos:

1. Quer gerar 2 pares de chaves diferentes (i.e., para diferentes objetivos);
2. Quer chaves RSA;
3. Quer chaves com 2048 bits;
4. Com um prazo de validade de 2 anos (escreve-se `2y`);
5. O nome de utilizador pode ser o seu ou um inventado;
6. O endereço de e-mail pode ser o seu ou um inventado;
7. No comentário escreva `Aula laboratorial 9`;
8. A palavra-passe escolhida deve ter **todos** os caracteres **diferentes**, um ou mais números, um **caracter especial**, letras **maiúsculas** e **minúsculas**, e **não** conter **nomes** nem **datas**. Coloque uma palavra-passe que consiga recordar adiante.

Q5.: Quais os dois objetivos diferentes dos dois pares de chaves que acabou de criar?
☐ Confidencialidade (cifra).
☐ Autenticação (assinatura-digital).
☐ Compressão.
☐ Integridade.
☐ Anonimato.

Q6.: Para além da RSA, qual o outro tipo de cifra de chave pública que pode ser usado no GPG?
☐ *Advanced Encryption Standard*.
☐ ElGamal.
☐ Criptografia sobre Curvas Elípticas.

Tarefa 3 *Task 3*

É possível que a aplicação avise que não tem entropia suficiente e lhe peça para continuar a trabalhar normalmente, até que ela gere a chave. Se quiser ver o ficheiro onde a aplicação está a ir buscar caracteres aleatórios, experimente emitir

```
$ cat /dev/random
```

no terminal, e observar atentamente o *output* do comando durante alguns instantes. Se precisar de aleatoriedade, experimente mexer o rato, abrir o *gedit* ou o *browser* e escrever algum texto, com ou sem sentido. **Q7.: Nota alterações no ficheiro `/dev/random`/ à medida que mexe o rato ou escreve?**
☐ Sim, noto. ☐ Não, não mexe nada.
☐ No meu sistema nem preciso fazer nada para ver a atividade imposta pelo sistema no ficheiro.

Q8.: Em que eventos é que o sistema operativo se baseia para popular a piscina de entropia que alimenta o `/dev/random`[2]?
☐ Movimentos e ações do rato.
☐ Introdução de dados pelo teclado.
☐ *Interrupts* ao processador.
☐ *Webcam* do utilizador.
☐ Operações de leitura / escrita no disco.
☐ Na resolução e claridade do monitor.

Q9.: Experimentou fazer `$ cat /dev/urandom`?
☐ Não. E nem vou fazer.
☐ Não, mas vou fazer.
☐ Sim, e creio ter o mesmo comportamento que o anterior.
☐ Sim, mas este não pára (não bloqueia) à espera de eventos.

Q10.: Acha que é seguro gerar chaves de cifra ou de assinatura digital a partir do `/dev/random`?
☐ Acho que é muito seguro.
☐ Acho que é muito seguro, mas eu tinha uma ideia melhor para fazer isto, nomeadamente:

_____

_____

☐ Acho que é razoavelmente seguro.
☐ Acho que é inseguro.

2 Analisar os Porta-Chaves

Analysing the Keyrings

Se efetuou devidamente a parte anterior do guia, o GPG criou dois pares chaves, que são guardados em:
☐ um porta-chaves. ☐ dois porta-chaves.

Para ver o conteúdo do porta-chaves público, pode usar o seguinte comando:

```
$ gpg --list-keys
```

Q11.: E para ver o porta-chaves privado, que co-

[2] O artigo em `http://www.suse.de/~thomas/papers/random-analysis.pdf` ou a dissertação em `http://www.di.ubi.pt/media/_ficheiros/dissertacoes/msc/m4705_diogo_fernandes.pdf` (página 26) podem ajudar a responder a esta pergunta.

mando deve usar?

$ _____

Q12.: Quantas chaves há dentro de cada porta-chaves?
☐ 1 chave ☐ 2 chaves ☐ 3 chaves ☐ 4 chaves

3 Exportar e Partilhar Chaves

Export and Share Keys

Tarefa 4 *Task 4*

Para que alguém possa enviar mensagens cifradas ou verificar a assinatura de determinado utilizador, é necessário que este exporte e partilhe a sua chave pública. O seguinte comando exporta a chave pública para um ficheiro *armored* (i.e., codificado na Base64) com o seu número de aluno(a):

```
$ gpg --export --armor --output
pub-keys-numero-aluno.pem
```

Quando bem sucedido, este comando cria um ficheiro (`pub-keys-numero-aluno.pem`) que pode ser enviado como anexo a um *e-mail* ou cujo conteúdo pode ser colado como assinatura do mesmo.

Envie este ficheiro ao(à) seu(ua) colega do lado...

Q13.: Precisa tomar alguma precaução no envio deste ficheiro?
☐ Creio que não.
☐ Com confiança: não!
☐ Preciso cifrar este ficheiro.
☐ Devo dividir este ficheiro ao meio e enviá-lo por dois canais independentes.

Tarefa 5 *Task 5*

Q14.: Já verificou o conteúdo do ficheiro criado? Quais os caracteres que lá encontrou?
☐ Caracteres de `A` a `Z`.
☐ Caracteres de `!` a `)`.
☐ Caracteres de `a` a `z`.
☐ Caracteres de `0` a `9`.
☐ Caracteres = e `-`.
☐ Caracteres de = a `/`.

Tarefa 6 *Task 6*

Após receber a chave pública enviada por outro utilizador, pode adicioná-la ao seu porta-chaves. **Q15.: A que porta-chaves é que vai adicionar esta chave?**
☐ Ao porta-chaves público.
☐ Ao porta-chaves privado.
☐ Ao porta-chaves que me saiu a semana passada quanto joguei numas senhas no café da esquina, e que é do *"mê Sporting"*.

Q16.: Qual o comando que vai usar para importar a chave?

$ _____

Tarefa 7 *Task 7*

Não se esqueça de voltar a verificar os portas-chaves no fim. **Q17.: Quantas chaves tem o porta-chaves privado?**
☐ As mesmas que antes.
☐ Surpreendentemente, menos que antes.
☐ Surpreendentemente, mais que antes.

4 Serviços de Confidencialidade e Autenticação

Confidentiality and Authentication Services

Tarefa 8 *Task 8*

Crie um ficheiro com uma mensagem, dirigida ao colega de quem tem a chave (e.g., `$ echo "o meu clube é o maior" > msg.txt`).
No fim, assine e cifre a mensagem:

```
$ gpg --armor -se msg.txt
```

O comando anterior tem 3 opções (`--armor`, `-s` e `-e`). Faça corresponder, usando números, os objetivos a cada uma das opções indicadas:

___ `--armor` ___ `-s` ___ `-e` ___ ϕ

1. Opção que pede ao GPG para cifrar.
2. Opção que pede ao GPG para assinar digitalmente.
3. Opção que garante que a mensagem está blindada contra escutas.
4. Opção que codifica a mensagem em Base64.
5. Opção que pede ao GPG para comprimir a mensagem antes da enviar.

Ao introduzir o comando anterior, o programa GPG vai interagir com o utilizador para pedir algumas informações. **Q18.: Acha que vai pedir a palavra-passe que guarda o porta-chaves privado?**
☐ Claro. ☐ Neste caso, não é preciso.
Use o espaço seguinte para colocar uma justificação da sua resposta:

Nota: quando o programa pedir os recipientes da mensagem, basta indicar o nome ou o email do(a) seu(ua) colega (que lhe enviou a chave), para que o programa escolha automaticamente as chaves. Note também que dava para adicionar mais do que um nome aos recipientes, e que **o programa lhe diz que não há evidências de que a chave que está a utilizar pertence realmente ao seu colega... Q19.: Por que é que o programa dá este aviso?**
☐ Porque o programa não é inteligente, e não sabe o que é a confiança.
☐ Porque nunca disse ao programa que confiava nesse utilizador e nas chaves dele(a).
☐ Porque nunca assinei nenhuma destas chaves com a minha chave privada.

Tarefa 9 *Task 9*

Depois de receber um ficheiro cifrado e assinado, pode decifrá-lo e verificar simultaneamente a assinatura, submetendo o seguinte comando:

```
$ gpg ____ msg.txt.asc
```

Q20.: Que opção ou opções faltam no comando anterior?
☐ `-armor` ☐ `-k` ☐ `-d` ☐ `--decrypt`
☐ `-s` ☐ `--verify` ☐ `--sign` ☐ `--encrypt`

Q21.: Quando decifrou a mensagem do seu colega, o GPG deu algum aviso acerca da autenticidade da chave usada?
☐ Sim, emitiu um aviso.
☐ Não disse nada. Devia dizer?

5 Assinar uma Chave

Sign a Key

O PGP define que, quando um utilizador confia numa chave de outra pessoa (i.e., confia uma chave pertence, de facto, à pessoa que diz possuí-la), a deve assinar com a sua chave privada. A assinatura de uma chave pública consegue-se através do seguinte comando:

```
$ gpg --sign-key nome_utilizador
```

O comando acima vai pedir-lhe a palavra-passe submetida na tarefa 2. **Q22.: Porque?**
☐ Porque o programa precisa aceder ao porta-chaves privado.
☐ Porque o programa precisa aceder ao porta-chaves público.
☐ Porque o programa precisa gerar novas chaves.

Depois disto, pode verficar as chaves e respetivas assinaturas usando o comando:

```
$ gpg --list-sigs
```

Tarefa 10 *Task 10*

Depois de assinar a chave do(a) colega, volte a decifrar a mensagem que recebeu dele(a). **Q23.: O GPG emitiu algum aviso relacionado com a confiança ou autenticidade da chave utilizada?**
☐ Sim, emitiu.

Q24.: Por curiosidade, como se elimina uma chave do GPG?
☐ `$ gpg --delete-key name`
☐ `$ gpg --drop-key name`
☐ `$ gpg --export-key name`

Tarefa 11 *Task 11*

Depois de se assinar uma chave, é boa política exportar essa chave e a sua assinatura, enviando-a para o titular da mesma, para que este(a) possa publicitar o facto de que há quem confie que aquela chave é, de facto, dele(a). Emita o comando que permite exportar a chave e a assinatura:

6 Ajustar a *Web-of-Trust*

Tweaking the Web-of-Trust

Tarefa 12 *Task 12*

O comando `$ gpg --update-trustdb` permite editar a **base de dados de confiança** depositada em

chaves e utilizadores (i.e., editar a *Web-of-Trust*). Procure explorar esta funcionalidade.

Quando emite o comando, deve conseguir ver imediatamente qual é a política de confiança que está a ser usada por defeito na sua instalação do programa. **Q25.: Quais das seguintes opções refletem essa política?**

☐ 5 chaves com confiança marginal.
☐ 3 chaves com confiança marginal.
☐ 1 chaves com confiança marginal.
—
☐ 2 chaves com confiança absoluta.
☐ 1 chave com confiança absoluta.
☐ 0 chaves com confiança absoluta.

Ao fazer a atualização da base de dados, dê confiança marginal à chave do seu(ua) colega.

Tarefa 13 *Task 13*

Verifique o *id* da chave do(a) seu(ua) colega. Use o comando

```
$ gpg --edit-key id
```

para editar a chave novamente, e tentar mudar a confiança que deposita nas chaves que vêm assinadas por ele(a).

Q26.: Qual a opção que permite exportar chaves PGP para um servidor?

☐ `--server-side-keys`
☐ `--export-keys`
☐ `--server-keys`
☐ `--send-keys`

Q27.: Qual a opção que permite importar chaves PGP a partir de um servidor?

☐ `--server-side-keys`
☐ `--import-keys`
☐ `--server-keys`
☐ `--recv-keys`

Tarefa 14 *Task 14*

Antes de terminar, considere ainda as seguintes questões e cenários. Assuma que havia recebido duas chaves públicas de dois utilizadores diferentes. Uma das chaves vinha com 10 assinaturas e outra vinha com 2 assinaturas. Esteve a verificar o seu chaveiro público, e reparou que apenas confiava marginalmente em 2 utilizadores que assinaram a chave que vinha com 10 assinaturas. Para o segundo caso, reparou que tinha confiança absoluta num dos utilizadores que havia assinado a chave, e confiança marginal no outro utilizador.

Q28.: Dado as respostas que deu na secção anterior, o que pode dizer acerca da confiança que o GPG terá na chave com 10 assinaturas?

☐ Que o GPG confiará absolutamente nessa chave.
☐ Que o GPG confiará marginalmente nessa chave.
☐ Que o GPG não deposita qualquer confiança nessa chave.

Q29.: A sua instância do GPG confia absolutamente na chave com as duas assinaturas?

☐ Sim, sem sombra de dúvidas.
☐ Não.

Tarefa 15 *Task 15*

Considere explorar melhor todas as funcionalidades do GPG (e do PGP).