# Aula TP - 19/Fev/2018

Cada grupo deve colocar a resposta às perguntas dos seguintes exercícios na área do seu grupo no Github até ao final do dia 27/Fev/2018. Por cada dia de atraso será descontado 0,15 valores à nota desse trabalho.

Note que a máquina virtual disponibilizada pode ser utilizada para fazer estes exercícios.

## Exercícios

### 1. Assinaturas cegas (*Blind signatures*) baseadas no Elliptic Curve Discrete Logarithm Problem (ECDLP)

Para este ponto necessita de copiar os ficheiros em TPraticas/Aula3 para a conta do utilizador *user* na máquina virtual. Sugere-se que copie esses ficheiros para a diretoria `/home/user/Aulas/Aula3`.

Nota: A descrição detalhada da técnica de assinatura cega que é utilizada neste exercício encontra-se neste paper

#### Experiência 1.1

Como estamos a falar em assinatura cega baseada em curvas elípticas, comecemos por gerar um par de chaves e certificado, utilizando o openssl.

Para isso, efetue os seguintes comandos:

- `openssl ecparam -name prime256v1 -genkey -noout -out key.pem`
  - gera o par de chaves para o ficheiro key.pem, utilizando uma curva elíptica do tipo prime256v1
- `openssl req -key key.pem -new -x509 -days 365 -out key.crt`
  - gera o certificado x509 com uma validade de 365 dias para o ficheiro key.crt

#### Experiência 1.2

Execute a assinatura cega, de acordo com as fases identificados na aula teórica (cf. slides 12 a 14 da aula teórica):

- Inicialização
- Ofuscação
- Assinatura
- Desofuscação
- Verificação

#### Pergunta P1.1

Como foi visto na aula teórica, a assinatura cega tem três participantes que participam em fases diferentes (cf. slide 11 da aula teórica):

- Requerente - efetua a fase de ofuscação e desofuscação,
- Assinante - efetua a fase de Inicialização e Assinatura,

- Verificador - efetua a fase de Verificação.

Pretende-se que altere o código fornecido para a experiência 1.2, de forma a simplificar o input e output, do seguinte modo (pode adicionar outras opções, se assim o desejar):

- Assinante:
  - `init-app.py`
    - devolve o R' (i.e., pRDashComponents)
  - `init-app.py -init`
    - inicializa as várias componentes (InitComponents e pRDashComponents) e guarda-as (por exemplo, em ficheiro do assinante)
  - `blindSignature-app.py -key <chave privada> -bmsg <Blind message>`
    - devolve s (i.e., Blind Signature)
- Requerente:
  - `ofusca-app.py -msg <mensagem a assinar> -RDash <pRDashComponents>`
    - devolve m' (i.e., Blind message) e guarda as restantes componentes (Blind components e pRComponents) em ficheiro do requerente
  - `desofusca-app.py -s <Blind Signature> -RDash <pRDashComponents>`
    - devolve s' (i.e., Signature)
- Verificador:
  - `verify-app.py -cert <certificado do assinante> -msg <mensagem original a assinar> -sDash <Signature> -f <ficheiro do requerente>`
    - devolve informação sobre se a assinatura sDash sobre a mensagem msg é ou não válida.

# 2. Protocolo SSL/TLS

### Experiência 2.1

Vá ao site www.ssllabs.com e efetue o *SSL Server test* para o site do Governo Português (https://www.portugal.gov.pt/).

Analise o resultado.

### Pergunta P2.1

Cada grupo indicado abaixo deve efetuar o teste *SSL Server test* aos sites indicados (que têm de obrigatoriamente funcionar sobre HTTPS) e responder às respetivas perguntas:

- Grupo 1 - Escolha três sites de Universidades Portuguesas.
  1. Anexe os resultados do *SSL Server test* à sua resposta.

2. Analise o resultado do *SSL Server test* relativo ao site escolhido com pior rating. Que comentários pode fazer sobre a sua segurança. Porquê?
3. É natural que tenha sido confrontado com a seguinte informação: "*This site works only in browsers with SNI support.*". O que significa, para efeitos práticos?

- Grupo 2 - Escolha três sites de Universidades Europeias, não Portuguesas.

  1. Anexe os resultados do *SSL Server test* à sua resposta.
  2. Analise o resultado do *SSL Server test* relativo ao site escolhido com pior rating. Que comentários pode fazer sobre a sua segurança. Porquê?
  3. É natural que tenha sido confrontado com a seguinte informação: "*HTTP Strict Transport Security (HSTS) with long duration deployed on this server.*". O que significa, para efeitos práticos?

- Grupo 3 - Escolha três sites de Universidades não Europeias.

  1. Anexe os resultados do *SSL Server test* à sua resposta.
  2. Analise o resultado do *SSL Server test* relativo ao site escolhido com pior rating. Que comentários pode fazer sobre a sua segurança. Porquê?
  3. É natural que tenha visto a seguinte informação: "*DNS CAA*". O que significa, para efeitos práticos?

- Grupo 4 - Escolha três sites de Ministérios do Governo Português.

  1. Anexe os resultados do *SSL Server test* à sua resposta.
  2. Analise o resultado do *SSL Server test* relativo ao site escolhido com pior rating. Que comentários pode fazer sobre a sua segurança. Porquê?
  3. É natural que tenha reparado na seguinte informação: "*DROWN*" na secção de detalhe do protocolo. O que significa, para efeitos práticos?

- Grupo 5 - Escolha três sites de Ministérios de Governos Europeus, não portugueses.

  1. Anexe os resultados do *SSL Server test* à sua resposta.
  2. Analise o resultado do *SSL Server test* relativo ao site escolhido com pior rating. Que comentários pode fazer sobre a sua segurança. Porquê?
  3. É natural que tenha reparado na seguinte informação: "*BEAST attack*" na secção de detalhe do protocolo. O que significa, para efeitos práticos?

- Grupo 6 - Escolha três sites de Ministérios de Governos não Europeus.

  1. Anexe os resultados do *SSL Server test* à sua resposta.
  2. Analise o resultado do *SSL Server test* relativo ao site escolhido com pior rating. Que comentários pode fazer sobre a sua segurança. Porquê?
  3. É natural que tenha reparado na seguinte informação: "*POODLE (SSLv3)*" na secção de detalhe do protocolo. O que significa, para efeitos práticos?

- Grupo 7 - Escolha três sites de Câmaras Municipais Portuguesas.

  1. Anexe os resultados do *SSL Server test* à sua resposta.
  2. Analise o resultado do *SSL Server test* relativo ao site escolhido com pior rating. Que comentários pode fazer sobre a sua segurança. Porquê?
  3. É natural que tenha reparado na seguinte informação: "*POODLE (TLS)*" na secção de detalhe do protocolo. O que significa, para efeitos práticos?

- Grupo 8 - Escolha três sites de Bancos Portugueses (ou sites de Bancos estrangeiros em .pt).
    1. Anexe os resultados do *SSL Server test* à sua resposta.
    2. Analise o resultado do *SSL Server test* relativo ao site escolhido com pior rating. Que comentários pode fazer sobre a sua segurança. Porquê?
    3. É natural que tenha reparado na seguinte informação: "*Downgrade attack prevention*" na secção de detalhe do protocolo. O que significa, para efeitos práticos?
- Grupo 9 - Escolha três sites de Bancos a operar na Europa (i.e., sites com domínios europeus, desde que não .pt).
    1. Anexe os resultados do *SSL Server test* à sua resposta.
    2. Analise o resultado do *SSL Server test* relativo ao site escolhido com pior rating. Que comentários pode fazer sobre a sua segurança. Porquê?
    3. É natural que tenha reparado na seguinte informação: "*Heartbleed (vulnerability)*" na secção de detalhe do protocolo. O que significa, para efeitos práticos?
- Grupo 10 - Escolha três sites de Bancos a operar fora da Europa (i.e., sites com domínios não europeus).
    1. Anexe os resultados do *SSL Server test* à sua resposta.
    2. Analise o resultado do *SSL Server test* relativo ao site escolhido com pior rating. Que comentários pode fazer sobre a sua segurança. Porquê?
    3. É natural que tenha reparado na seguinte informação: "*Ticketbleed (vulnerability)*" na secção de detalhe do protocolo. O que significa, para efeitos práticos?
- Grupo 11 - Escolha três sites de empresas não bancárias cotadas na Bolsa Portuguesa e pertencentes ao PSI 20.
    1. Anexe os resultados do *SSL Server test* à sua resposta.
    2. Analise o resultado do *SSL Server test* relativo ao site escolhido com pior rating. Que comentários pode fazer sobre a sua segurança. Porquê?
    3. É natural que tenha reparado na seguinte informação: "*OpenSSL CCS vuln. (CVE-2014-0224)*" na secção de detalhe do protocolo. O que significa, para efeitos práticos?
- Grupo 12 - Escolha três sites de empresas não bancárias e não portuguesas cotadas na Euronext.
    1. Anexe os resultados do *SSL Server test* à sua resposta.
    2. Analise o resultado do *SSL Server test* relativo ao site escolhido com pior rating. Que comentários pode fazer sobre a sua segurança. Porquê?
    3. É natural que tenha reparado na seguinte informação: "*ROBOT (vulnerability)*" na secção de detalhe do protocolo. O que significa, para efeitos práticos?
- Grupo 13 - Escolha três sites de empresas cotadas no NASDAQ.
    1. Anexe os resultados do *SSL Server test* à sua resposta.
    2. Analise o resultado do *SSL Server test* relativo ao site escolhido com pior rating. Que comentários pode fazer sobre a sua segurança. Porquê?
    3. É natural que tenha reparado na seguinte informação: "*OpenSSL Padding Oracle vuln. (CVE-2016-2107)*" na secção de detalhe do protocolo. O que significa, para efeitos práticos?
- Grupo 14 - Escolha três sites de empresas cotadas no NYSE.

1. Anexe os resultados do *SSL Server test* à sua resposta.
2. Analise o resultado do *SSL Server test* relativo ao site escolhido com pior rating. Que comentários pode fazer sobre a sua segurança. Porquê?
3. É natural que tenha reparado na seguinte informação: "*Public Key Pinning*" na secção de detalhe do protocolo. O que significa, para efeitos práticos?

## 3. Protocolo SSH

Para este ponto necessita de instalar o ssh-audit na conta do utilizador *user* na máquina virtual. Sugere-se que efetue a seguinte sequência de comandos:

```
cd
```

```
mkdir Tools
```

```
cd Tools
```

```
git clone https://github.com/arthepsy/ssh-audit
```

```
cd ssh-audit
```

```
python ssh-audit.py
```

### Experiência 3.1

Utilize o ssh-audit para efetuar um teste ao servidor algo.paranoidjasmine.com, i.e.

```
python ssh-audit.py algo.paranoidjasmine.com
```

Analise o resultado.

### Pergunta P3.1

Cada grupo indicado abaixo deve utilizar o ssh-audit para efetuar teste aos sites indicados, que têm de obrigatoriamente ter o ssh (usualmente, na porta 22) ativo.

Nota 1: Para simplificar a resposta a esta pergunta deverá configurar uma conta em https://www.shodan.io/, já que após login pode fazer pesquisas fáceis sobre serviços disponíveis na Web. Por exemplo, para pesquisar por servidores ssh em Braga, poderá pesquisar por `port:22 country:pt city:braga`. Se quiser saber os servidores ssh da Universidade do Minho, pode pesquisar por `port:22 org:"Universidade do Minho"`.

Nota 2: Para pesquisar as vulnerabilidades de um produto software pode utilizar a pesquisa no site CVE details,

inserindo o nome do produto e a versão a pesquisar.

Cada Grupo deve escolher:

- Grupo 1 - Escolha dois servidores ssh de Universidades Portuguesas.
- Grupo 2 - Escolha dois servidores ssh de Universidades Europeias, não Portuguesas.
- Grupo 3 - Escolha dois servidores ssh de Universidades não Europeias.
- Grupo 4 - Escolha dois servidores ssh de empresas comerciais em Braga.
- Grupo 5 - Escolha dois servidores ssh de empresas comerciais no Porto.
- Grupo 6 - Escolha dois servidores ssh de empresas comerciais em Lisboa.
- Grupo 7 - Escolha dois servidores ssh de empresas comerciais em Madrid.
- Grupo 8 - Escolha dois servidores ssh de empresas comerciais em Paris.
- Grupo 9 - Escolha dois servidores ssh de empresas comerciais em Londres.
- Grupo 10 - Escolha dois servidores ssh de empresas comerciais em San Francisco.
- Grupo 11 - Escolha dois servidores ssh de empresas cotadas na Bolsa Portuguesa.
- Grupo 12 - Escolha dois servidores ssh de empresas não portuguesas cotadas na Euronext.
- Grupo 13 - Escolha dois servidores ssh de empresas cotadas no NASDAQ.
- Grupo 14 - Escolha dois servidores ssh de empresas cotadas no NYSE.

Responda aos seguintes pontos:

1. Anexe os resultados do ssh-audit à sua resposta.
2. Indique o software e versão utilizada pelos servidores ssh.
3. Qual dessas versões de software tem mais vulnerabilidades?
4. E qual tem a vulnerabilidade mais grave (de acordo com o *CVSS score* identificado no CVE details)?
5. Para efeitos práticos, a vulnerabilidade indicada no ponto anterior é grave? Porquê?