TP Class Assignment - 18/Feb/2018

Each group must answer the questions of the following exercises in the Github area of their group until the end of 27/Feb/2018. For each day of delay, 0.15 points will be deducted from the grade of this assignment.

Note that the virtual machine provided for this course can be used to solve these exercises.

Exercises

1. ECDLP-based Blind signatures

Please copy the files in the TPraticas/Aula3 to the user account *user* in the virtual machine. It is suggested that you copy these files to the `/home/user/Aulas/Aula3` directory.

Note: The detailed description of the blind signing technique used in this exercise can be found in this paper

Experience 1.1

Since this exercise is about blind signature based on elliptic curves, let's start by generating a key pair and certificate, using openssl (following commands):

- `openssl ecparam -name prime256v1 -genkey -noout -out key.pem`
  - generates the key pair into the key.pem file, using an elliptic curve of type prime256v1
- `openssl req -key key.pem -new -x509 -days 365 -out key.crt`
  - generates the x509 certificate with a 365-day validity period into the key.crt file

Experience 1.2

Perform the blind signature, according to the phases identified in the theoretical class (see slides 12 to 14 of the theoretical class):

- Initialization;
- Obfuscation/Blind;
- Signature;
- Unblind;
- Verification

Question P1.1

As seen in the theoretical class, the blind signature has three participants who participate in different phases (see slide 11 of the theoretical lesson):

- Requester - performs the Blinding and Unblinding phase,
- Signer - performs the Initialization and Signing phase,
- Verifier - performs the Verifying phase.

It is intended to change the code provided for experience 1.2 in order to simplify the input and output as follows (you can add other options if you wish):

- Signer:
    - `init-app.py`
        - returns R' (i.e., pRDashComponents)
    - `init-app.py -init`
        - initializes the different components (InitComponents and pRDashComponents) and saves them (for example, in a signer's file)
    - `blindSignature-app.py -key <private key> -bmsg <Blind message>`
        - returns s (i.e., Blind Signature)
- Requester:
    - `ofusca-app.py -msg <message to sign> -RDash <pRDashComponents>`
        - returns m' (i.e., Blind message) e gsaves the other components (Blind components e pRComponents) in a requester's file
    - `desofusca-app.py -s <Blind Signature> -RDash <pRDashComponents>`
        - returns s' (i.e., Signature)
- Verifier:
    - `verify-app.py -cert <signer certificate> -msg <message to sign> -sDash <Signature> -f <requester's file>`
        - returns information about whether the sDash signature on the msg message is valid.

2. SSL/TLS protocol

Question 2.1

Go to www.ssllabs.com and perform the *SSL Server test* for the Portuguese Government website (https://www.portugal.gov.pt/).

Analyze the result.

Question P2.1

Each group must test the *SSL Server test* for the designated sites (which must necessarily work on HTTPS) and answer the questions:

- Group 1 - Choose three Portuguese Universities sites.

1. Attach the results of the *SSL Server test* to your answer. 2. Analyze the result of the *SSL Server test* for the site with the worst rating. What comments can you make about its safety. Why? 3. In the result of the *SSL Server test*

you have the following information: "*This site works only in browsers with SNI support.*". What does it mean, for practical purposes?

- Group 2 - Choose three European Universities (non-Portuguese) sites.

  1. Attach the results of the *SSL Server test* to your answer.   2. Analyze the result of the *SSL Server test* for the site with the worst rating. What comments can you make about its safety. Why?   3. In the result of the *SSL Server test* you have the following information: "*HTTP Strict Transport Security (HSTS) with long duration deployed on this server.*". What does it mean, for practical purposes?

- Group 3 - Choose three non-European Universities sites.

  1. Attach the results of the *SSL Server test* to your answer.   2. Analyze the result of the *SSL Server test* for the site with the worst rating. What comments can you make about its safety. Why?   3. In the result of the *SSL Server test* you have the following information: "*DNS CAA*". What does it mean, for practical purposes?

- Group 4 - Choose three Portuguese state department (ministries) sites.

  1. Attach the results of the *SSL Server test* to your answer.   2. Analyze the result of the *SSL Server test* for the site with the worst rating. What comments can you make about its safety. Why?   3. In the result of the *SSL Server test* you have the following information in the protocol details section: "*DROWN*". What does it mean, for practical purposes?

- Group 5 - Choose three European non-Portuguese state department (ministries) sites.

  1. Attach the results of the *SSL Server test* to your answer.   2. Analyze the result of the *SSL Server test* for the site with the worst rating. What comments can you make about its safety. Why?   3. In the result of the *SSL Server test* you have the following information in the protocol details section: "*BEAST attack*". What does it mean, for practical purposes?

- Group 6 - Choose three non-European state department (ministries) sites.

  1. Attach the results of the *SSL Server test* to your answer.   2. Analyze the result of the *SSL Server test* for the site with the worst rating. What comments can you make about its safety. Why?   3. In the result of the *SSL Server test* you have the following information in the protocol details section: "*POODLE (SSLv3)*". What does it mean, for practical purposes?

- Group 7 - Choose three Portuguese city town hall sites.

  1. Attach the results of the *SSL Server test* to your answer.   2. Analyze the result of the *SSL Server test* for the site with the worst rating. What comments can you make about its safety. Why?   3. In the result of the *SSL Server test* you have the following information in the protocol details section: "*POODLE (TLS)*". What does it mean, for practical purposes?

- Group 8 - Choose three Portuguese Bank sites (ou foreign Bank sites under .pt).

  1. Attach the results of the *SSL Server test* to your answer.   2. Analyze the result of the *SSL Server test* for the site with the worst rating. What comments can you make about its safety. Why?   3. In the result of the *SSL Server test* you have the following information in the protocol details section: "*Downgrade attack prevention*". What does it mean, for practical purposes?

- Group 9 - Choose three European Bank sites (i.e., sites under an european domain, but not under .pt).

  1. Attach the results of the *SSL Server test* to your answer.   2. Analyze the result of the *SSL Server test* for the

site with the worst rating. What comments can you make about its safety. Why?   3. In the result of the *SSL Server test* you have the following information in the protocol details section: "*Heartbleed (vulnerability)*". What does it mean, for practical purposes?

- Group 10 - Choose three non-European Bank sites (i.e., sites under a non-european domain).

  1. Attach the results of the *SSL Server test* to your answer.   2. Analyze the result of the *SSL Server test* for the site with the worst rating. What comments can you make about its safety. Why?   3. In the result of the *SSL Server test* you have the following information in the protocol details section: "*Ticketbleed (vulnerability)*". What does it mean, for practical purposes?

- Group 11 - Choose three non-Bank company sites (companies listed in the PSI 20)

  1. Attach the results of the *SSL Server test* to your answer.   2. Analyze the result of the *SSL Server test* for the site with the worst rating. What comments can you make about its safety. Why?   3. In the result of the *SSL Server test* you have the following information in the protocol details section: "*OpenSSL CCS vuln. (CVE-2014-0224)*". What does it mean, for practical purposes?

- Group 12 - Choose three non-Bank and non-Portuguese company sites (companies listed in the Euronext stock exchange)

  1. Attach the results of the *SSL Server test* to your answer.   2. Analyze the result of the *SSL Server test* for the site with the worst rating. What comments can you make about its safety. Why?   3. In the result of the *SSL Server test* you have the following information in the protocol details section: "*ROBOT (vulnerability)*". What does it mean, for practical purposes?

- Group 13 - Choose three sites of companies listed in NASDAQ stock exchange.

  1. Attach the results of the *SSL Server test* to your answer.   2. Analyze the result of the *SSL Server test* for the site with the worst rating. What comments can you make about its safety. Why?   3. In the result of the *SSL Server test* you have the following information in the protocol details section: "*OpenSSL Padding Oracle vuln. (CVE-2016-2107)*". What does it mean, for practical purposes?

- Group 14 - Choose three sites of companies listed in NYSE stock exchange.

  1. Attach the results of the *SSL Server test* to your answer.   2. Analyze the result of the *SSL Server test* for the site with the worst rating. What comments can you make about its safety. Why?   3. In the result of the *SSL Server test* you have the following information in the protocol details section: "*Public Key Pinning*". What does it mean, for practical purposes?

3. SSH Protocol

If you are not using the virtual machine provided for this course, please install the ssh-audit tool in your computer, as follows:

```
cd
```

```
mkdir Tools
```

```
cd Tools
```

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

```
cd ssh-audit
```

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

Experience 3.1

Use the ssh-audit tool to test the algo.paranoidjasmine.com server, i.e.

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

Analyze the result.

Question P3.1

Each group must use the ssh-audit tool to test the designated sites, which must have ssh service (usually on port 22) active.

Note 1: To simplify your answer to this question you should set up an account at https://www.shodan.io/, in order to search services available on the Web. For example, to search for ssh servers in Braga, you can search for `port:22 country:pt city:braga`. If you want to know the ssh servers at University of Minho, you can search for `port:22 org:"University of Minho"`.

Note 2: To search for vulnerabilities in a software product you can use the search tool on the CVE details site, by entering the product name and version to search.

Tests to be performed by:

- Group 1 - Choose two Portuguese Universities ssh servers.
- Group 2 - Choose two European non-Portuguese Universities ssh servers.
- Group 3 - Choose two non-European Universities ssh servers.
- Group 4 - Choose two ssh servers from Braga companies.
- Group 5 - Choose two ssh servers from Porto companies.
- Group 6 - Choose two ssh servers from Lisbon companies.
- Group 7 - Choose two ssh servers from Madrid companies.
- Group 8 - Choose two ssh servers from Porto companies.
- Group 9 - Choose two ssh servers from London companies.
- Group 10 - Choose two ssh servers from San Francisco companies.
- Group 11 - Choose two ssh servers from companies listed in the Portuguese stock exchange.
- Group 12 - Choose two ssh servers from non-Portuguese companies listed in the Euronext stock exchange.

- Group 13 - Choose two ssh servers from companies listed in the NASDAQ stock exchange.
- Group 14 - Choose two ssh servers from companies listed in the NYSE stock exchange.

Answer the following questions:

1. Attach the ssh-audit results to your answer.
2. Specify the software and version used by each ssh server.
3. Which of these versions of software has the most vulnerabilities?
4. Which one has the most severe vulnerability (according to the *CVSS score* identified in CVE details)?
5. For practical purposes, is the vulnerability referred in the previous paragraph serious (security wise)? Why?