Hands on X.509 and Transport Layer Security (TLS) with scapy Lab

Santiago Ruano Rincón - Sandrine Vaton

2018

Credits

This laboratory is largely based on the work and code by Maxence Tury from ANSSI.

1 Introduction

This laboratory aims at improving knowledge about X.509 certificates and TLS by a practical work using scapy. I hope that, after this laboratory, you should have a better understanding on X.509 certificates' common features, and how TLS sessions are established under cryptography mechanisms, also relying on X.509.

Inspecting the content of X.509 certificates and TLS recorded sessions, this lab will also help you to understand how TLS guarantees different security properties, needed to protect users privacy when using different Internet protocols.

2 Scapy and the Jupyter notebooks

This lab relies on Scapy, a Python module that makes it possible to manipulate network packets. We will use it through three Jupyter notebooks:

- Notebook 1: X.509 certificates
- Notebook 2: TLS handshake overview
- Notebook 3: The lack of PFS (Perfect Forward Secrecy) as a danger to privacy

You can access the notebooks by the https://jupyterhub.telecom-bretagne.eu/ URL, logging in with your usual credentials. Inside the `notebooks` working directory, you will find `raw_data/` that stores different sets of files that will be used in each notebook:

```
raw_data/pki/
raw_data/tls_session_protected/
raw_data/tls_session_compromised/
```

There is an additional Notebook 0, with introductory information about TLS. The work will begin with Notebook 1.

> **Note:** Please, since we will be using a shared server, try to keep **running one notebook at a time**, **close and halt** each notebook when you are not using it to minimize the use of the server resources.

These notebooks are composes of cells. As you can see, one of the first required steps in each notebook is to import the scapy modules that you will need:

```
from scapy.all import *
```

> Follow the instructions and answer the questions found in each notebook. Please note some code cells include instructions or help as comments.

3 Notebook 1: X.509 certificates

This notebook looks at inspecting the content of X.509 certificates, and manipulating them with scapy. Certificates and their related private keys of a Certification Authority (CA) and a server are available at the `raw_data/pki/` directory. You will access their contents at different stages of the notebook.

4 Notebook 2: TLS handshake overview

In this notebook you will observe the different messages that compose a TLS (v1.2) handshake. TLS session messages have been recorded and stored at `raw_data/tls_session_protected/`.

5 Notebook 3: The lack of Perfect Forward Secrecy (PFS) in TLS

This notebook explores a potential flaw that could compromise the confidentiality of recorded sessions. You will review the exchange stored in `raw_data/tls_session_compromised/`, under the assumption that the server's private key has been compromised (**The server is the same than notebook 1**). The main goal of this notebook is to be aware of the security requirements to protect the session secrets that make it possible to encrypt the useful data. Compare this session against the protected exchange. As for the previous notebooks, you will find questions at the ending cell.