PKI using SSL

CS 337: Network Security
(Fall 2023) Due: 26 October -2023

Introduction

So far in this course, you've seen many cryptographic protocols, learned how they work, and how they may be attacked. One of the biggest issues we discussed, is how two principals can share keys in an untrusted environment to achieve their security objectives. Ex. How do we verify the ownership of a public key using the principals claimed identity?

For this course's project, we'll take a look a closer look at the Public-Key Infrastructure (PKI), which is a practical solution for the above problem. You'll gain first-hand experience on PKI using a lab created by Seed Labs, which is a project led by Professor Wenliang Du, with many of his students working on these labs and environments.

This lab covers the following topics:

- Public-key encryption
- Public-Key Infrastructure (PKI)
- Transport Layer Security (TLS), which is an updated and more secure version of SSL.
- Certificate Authority (CA) and root CA
- X.509 certificate and self-signed certificate
- Apache, HTTP, and HTTPS
- Man-in-the-middle attacks

Background

In this lab you'll be performing the following 6 Tasks:

1. Becoming a certificate authority (CA).
2. Creating a certificate.
3. Deploying the certificate in a web server.
4. Deploying certificate in an Apache-based HTTPS website.
5. Launching a Man in the Middle Attack.
6. Launching a Man in the Middle Attack using a compromised CA.

You'll find the full lab details and detailed steps on how to execute the tasks above, on the lab's webpage https://seedsecuritylabs.org/Labs_16.04/Crypto/Crypto_PKI/ . You will also find a link to an Ubuntu VM which has all the tools you'll need pre-installed, such as openssl and its libraries.

Submission

As mentioned in the lab description. You need to submit a detailed lab report to describe what you have done and what you have observed; you also need to provide explanation to the observations that are interesting or surprising. In your report, you need to answer all the questions listed in this lab.

If you have any questions or need assistance, kindly send me an email at Faaljumah@imamu.edu.sa

Note: *We take plagiarism very seriously. The project's level of difficulty is very reasonable, so make sure you do this project yourself. For that reason, please change the VM's wallpaper to picture with your name, make sure you work in a directory with your name ex. ~/FerasJ , and make sure your terminal or browser window doesn't cover the entire screen when you take a screenshot.*