Exprimenting with X.509 Public Key Infrastructure

Hui Chen
Computer Science
Virginia State University, Virginia 23806
E-mail: huichen (AT) ieee.org

Written on September 21, 2015
Lastly revised on October 14, 2015
Revision: 138:053429736bb6

The project is based on the "Crypto Lab Public-Key Cryptography and PKI" lab developed by Professor Wenliang Du at Syracus University [1]. In this document, the lab is referred to as the PKI lab and the associated lab document is referred to as the PKI lab manual.

The objective as stated in the lab is to help readers gain familiarity with concepts pertaining to the X.509 Public Key Infrastructure (PKI) including public key cryptography, digital signature, X.509 public-key certificate, certificate authority, authentication based on PKI and with the tools and software necessary to set up PKI.

1 Experiment Environment

The SEED lab provides a few Ubuntu Virtual Machines for this lab. The virtual machines have lots of software installed and can be used to work with a collection of security labs, called the SEED labs created by Professor Wenliang Du. However, the footprints of the virtual machines are also quite large. Considering some students' own computers do not have much spare disk space and do not have much RAM, the instructor prepares a Debian Linux virtual machine for this PKI lab. The virtual machine is smaller in size (about 200MB in a compressed archive) and use much less RAM (64 MB). The tools and programs needed for the lab have already been loaded to the Debian Linux virtual machine. The instructor refers this virtual machine to as the Debian Linux virtual machine. Download the Debian Linux virtual machine from either Dropbox or OneDrive.

The Debian Linux virtual machine is in a 7-zip compressed archive file. You can use the 7-zip file archiver to extract the virtual machine.

2 Assignment

Students are required to complete all the tasks in the PKI lab manual, i.e., Tasks 1 - 6. Note that the instructor provides below a few clarifications on the Lab Environment and Tasks described in the PKI lab manual.

2.1 Lab Environment

The OpenSSL has already installed on the Debian Linux virtual machine. You should skip Section Lab Environment in the PKI lab manual. The TCP client and server programs to be used in Task 4 have also been loaded to the Debian Linux virtual machine.

2.2 Task 1

The configuration file of the OpenSSL is located at the directory `/home/debian/openssl` instead of `/home/seed/openssl-1.0.1`. Replace the later by the former in the PKI lab manual when you follow the provided Debian Linux virtual machine.

2.3 Task 3

First, let us clarify two terms. The computer that runs the VirtualBox software is a *virtual machine host*, or a *VM host*, or a *host* when the context in which the term appear warrants no ambiguity. The Debian Linux virtual machine that runs inside VirtualBox is a *virtual machine guest* or a *guest*.

The instructor has the following recommendations.

- Skip the step in which `PKILabServer.com` is added to `/etc/hosts`.
- Run Mozilla Firefox in the host and the OpenSSL server at the guest when you work on Task 3.
- In Mozilla Firefox, enter IP address of the guest instead of PKILabServer.com. To find out the IP address of the guest, issue the following command in the guest,

  ```
  ip address show eth1
  ```

  The IP address is in decimal-dot-notation, e.g., 192.168.56.109. Note that yours may vary.

  Be aware that you must explicitly type the protocol *https* in the address bar as the PKI lab manual states.

  For instance, if your IP address is 192.168.56.109, you should enter `https://192.168.56.109:4433`.
- Firefox will display an error message indicating "This Connection is Untrusted" as shown in Figure 1.

  As stated in the PKI lab manual, to address the problem, you need to let your Firefox to trust your certificate authority by loading `ca.crt` generated in Task 1 into Firefox.

  Since you run Firefox in the host and the `ca.crt` in the guest, you will have to using an "out-of-band" channel to retrieve the certificate file and load it to Firefox.

  Alternatively, you can simply click on "I Understand the Risks" and then "Add Exception" to load the certificate without using an "out-of-band" channel to retrieve the file.

3 Tasks 4 – 6

The PKI lab manual does not provide detailed steps how you may complete the tasks. These are the challenges designed for you. You should find out how you may complete the tasks using your own research.

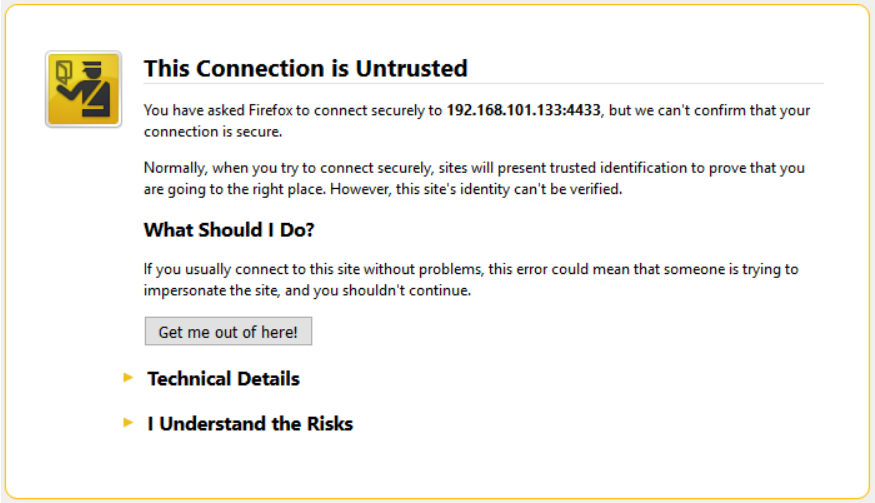

Figure 1: Firefox displays a "untrusted connectin" error.

4 Submission

As stated in the PKI lab manual, "[y]ou 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 [the PKI lab manual]."

In addition, answer the following questions in your lab report based on your research.

1. Explain concisely TLS and SSL.

2. Tasks 1 and 2 are performed on a single machine. Is this a typical operation in practice? Identify a Certificate Authority and use its website to investigate how a SSL certificate is being requested and issued.

3. What are the difference between "Domain Validated" certificates, "Organization Validated" certificates, and "Extended Validated" certificates? Identify a Certificate Authority and use its website to investigate how an organization or an individual may obtain "Domain Validation", or "Organization Valiadtion", or "Extended Validation".

4. Download a Root Certificate recognized by Firefox and show that it is a self-signed certificate using OpenSSL.

5. Explain the difference between Root Certificate Authority and Intermediate Certificate Authority. Can you create the certificate for an Intermediate Certificate Authority using OpenSSL? Explain how and show an example using your own self-signed root certificate created in Task 1.

6. Tasks 4 demonstrates a TCP client program and a TCP server program. The client needs to authenticate the server. This server authentication is done using the created public-key certificate. Much software has been developed using SSL certificate for the same purpose.

With your research, name two pieces of commonly used software that use SSL certificates for authentication, briefly describe how one may obtain a public key certificate from a Certificate Authority, and deploy the certificate for the software to use.

References

[1] Wenliang Du and Ronghua Wang. Seed: A suite of instructional laboratories for computer security education. *J. Educ. Resour. Comput.*, 8(1):3:1–3:24, March 2008.