Exploring Public Key Certificates

The goal of this lab is to familiarize the student with public key certificates and the use of SSL/TLS.

Task 1. Exploring Given Website Certificates

A. Boot your Linux system or VM. If necessary, log in and then open a terminal window and cd to the labtainer/labtainer-student directory. The pre-packaged Labtainer VM will start with such a terminal open for you. Then start the lab:

```
labtainer pubkey
```

Note the terminal displays the paths to two files on your Linux host:

1) This lab manual

2) The lab report template

3) The lab worksheet

On most Linux systems, these are links that you can right click on and select "Open Link". **If you chose to edit the lab report or worksheet on a different system, you are responsible for copying the completed documents back to the displayed path on your Linux system before using "stoplab" to stop the lab for the last time.**

Press <enter> to start the lab. A Firefox browser will open automatically for your use in this lab.

Items #1 through #4 provide four tables you need to fill out. Each table has five URLs that all start with "http**s**". This prefix causes the SSL/TLS protocol to kick in, which results in the transfer of a PKI certificate from the associated website to your browser. You are going to be examining these certificates.

For each of the URLs in these tables, do the following:

1. Visit the URL via the browser (using http**s** as the prefix).
2. Click on the icon at the left-hand side of the address field.
3. Select the '>' symbol in the popup.
4. Select **More information** from the pop-up window.
5. Select the **Security** icon.
6. Select **View Certificate** from the new window.
7. Select the **Details** tab.
8. From the **Certificate Fields** area, select the field being requested in the table.

9. Take the information from the **Field Value** area and transfer it to the table.
10. Select **Close** when you are done with the certificate.

Fill in the worksheet table by visiting all twenty URLS. [The second-to-last column only applies to RSA keys. In other words if the “Key Algorithm” is something else, then that column does not apply.]

Task 2. Exploring Other Website Certificates

Refer to the table in item #5 of the Worksheet.

Visit 5 other sites that you normally frequent using “http” to get there, but this time use the “http**s**” prefix instead. Complete the table in the worksheet as you go. If HTTPS is not supported, then a certificate will not be available to investigate. An answer of “Depends” should be given if the site only supports HTTPS sometimes. For example, some websites support HTTPS only when you want to actually buy something, such as hitting the “check out” button.

Note that this counts as your “experimentation”.

Exit the browser when you are done completing the tables.

Submission

After finishing the lab, go to the terminal on your Linux system that was used to start the lab and type:

```
stoplab pubkey
```

If you modified the lab report or worksheet on a different system, you must copy those completed files into the directory paths displayed when you started the lab, and you must do that before typing “stoplab”. When you stop the lab, the system will display a path to the zipped lab results on your Linux system. Provide that file to your instructor, e.g., via the Sakai site.