CryptoWorks21

FUNDAMENTALS OF NETWORK SECURITY

PRACTICAL — TRANSPORT LAYER SECURITY (TLS) AND WIRESHARK

In this exercise, you will examine the operation of the Transport Layer Security (TLS) protocol using the Wireshark packet sniffing application.

Step 1: Inspect certificate in your web browser

1. Visit an encrypted webpage in your web browser, for example, https://uwaterloo.ca/.
2. Click on the security icon in your web browser's location bar. Depending on the browser, this may be a lock icon or the "https" symbol.
3. Different browsers show different information. Firefox and Opera often show the most detailed information, including information on the server's certificate and the encryption mode used. (Google Chrome has, for some reason, reduced the amount of information they show.)
4. Take a look at the certificate.
    a. Who is the certificate authority that issued the certificate?
    b. What public key algorithm is used?
    c. What type of validation did the certificate authority use?

Step 2: Install Wireshark

You will make use of the Wireshark software, which is available for Windows, Mac, and Linux. You can download it from http://www.wireshark.org. Once you have installed it, proceed with the steps below. Note that on Mac OS X, you will also need to install X11, which you can download from http://xquartz.macosforge.org/.

Step 3: Capture packets

1. Launch Wireshark.
2. Initiate a packet capture on your main outgoing network interface. On the main Wireshark screen, select your network interface (for example, en0), and then click "Start". Note that on Linux or Mac, you may need to run Wireshark as root to be able to capture packets. (There is a way to run without root privileges, but that requires a bit of work.)
3. Visit an unencrypted webpage in your web browser, for example, http://www.utm.toronto.edu/.
4. Visit an encrypted webpage in your web browser, for example, https://uwaterloo.ca.
5. Switch back to Wireshark and stop the packet capture.

You can now filter the Wireshark packet capture to see what the network traffic looks like.

- If you filter for "http", you should see the various connections that were made to the unencrypted website.

- If you filter for "ssl", you should see the various connections that were made to the encrypted website. You will see the various TLS messages sent—ClientHello, ServerHello, etc.—and you can drill down to the see the contents of those messages in the bottom half of the Wireshark window. Can you figure out which ciphersuite was negotiated?
- Notice as well that you cannot read the body of the requests that were sent to the encrypted website. They only appear as "Application data" in the TLS filter. This is all that an eavesdropper on the Internet would see.

TO SUBMIT

1. Answers to the questions from step 1:
    a. Who is the certificate authority that issued the certificate?
    b. What public key algorithm is used?
    c. What type of validation did the certificate authority use?
2. Screenshots demonstrating your captures for Step 3 parts 3 and 4. For https://uwaterloo.ca, include a screenshot of the Wireshark capture that shows which ciphersuite was negotiated between your browser and the web server.