MAS433 Cryptography: Assignment 2

Submission Instructions:

1. Submission deadline: 10PM, 06 November 2011.
2. You need to email your answers to the instructor (wuhj@ntu.edu.sg) with the email subject "MAS433 Assignment 2".

Questions: TLS/SSL is used to protect the communication between the NTU webmail server and its users.

1. Briefly describe the difference between TLS and SSL.
2. Briefly describe the contents in a public key certificate.
3. Describe the details of the simple TLS handshake.
4. When you connect to the webmail server,
   - 4.1 ClientHello.
     - 4.1.1 What is the browser that you are using?
     - 4.1.2 What is the highest TLS protocol version your browser can support?
     - 4.1.3 What are the CipherSuites supported by your browser?
   - 4.2 ServerHello.
     - 4.2.1 What is the TLS version being used between the webmail server and your browser?
     - 4.2.2 What is the CipherSuite being used between the webmail server and your browser?
   - 4.3 Public key certificate.
     - 4.3.1 What are the cryptosystems being used for generating the public key certificate of the NTU webmail server?

4.3.2 What is the certificate authority of the NTU webmail server?

4.3.3 What is the validity period of the current public key certificate of the NTU webmail server?

4.3.4 What is the public key of the NTU webmail server? Is it strong?

4.3.5 (Bonus Question) What is the private key of the NTU webmail server?

4.4 Explain why the public key certificate is needed in TLS/SSL.

4.5 List the cryptosystems that are used to protect the communication between your computer and the NTU webmail server.

4.6 Briefly describe how the secret keys are established between your computer and the webmail server.

Hints:

1. Google
2. Wikipedia: TLS/SSL, public key certificate, ...
3. If you are using Internet Explorer to access webmail, you may click the "lock" icon near the address bar.
4. You need to install a network traffic analyzer to capture and analyze the internet traffic between your computer and the NTU webmail server.

   3.1 You may install the network analyzer "WIRESHARK" on your computer. You can install all the features of WIRESHARK. You may search the tutorial of WIRESHARK for detail instruction on how to use WIRESHARK. Some brief introduction is given below.

   3.2 After starting the WIRESHARK for the first time, from the menu, click "capture", click "options", unmark "capture packets in promiscuous mode", then click "start", then WIRESHARK starts capturing the packets.

   3.3 To capture the communication data between your computer and the eventure server, you may start the capturing of the WIRESHARK, then type the URL of eventure server in your browser, press "enter" key, then you can stop the capturing of the WIRESHARK, and start analyzing those packets.

3.4 After packet capturing, the WIRESHARK window is divided into three parts. The upper part lists those packets, the middle part shows the "translated" content of each packet (you can find the detailed packet information there), the lower part gives the hexadecimal data in each packet.

3.5 To simply the analysis, you can organize the order of packets by clicking "protocol" in the "WIRESHARK" window. You only need to analyze those TLS/SSL packets.