FIT1047 Tutorial 11

Topics

- TLS, HTTP, HTTPS
- Certificates for HTTPS

Instructions

- The tasks are supposed to be done in groups.

Task 1: TLS, HTTP, HTTPS

For this task you need to use *Wireshark* again in order to look at three different examples of recorded network traffic. All three examples show parts of the communication between a client and a webserver.

Before you start, get files Example1.pcap, Example2.pcap and Example3.pcap from Moodle.

1.a Start Wireshark and open Example1.pcap.

- Can you identify the domain name of the server?
- Which protocols are used on application layer?
- Now open Chrome and type in the address that you have identified, using the protocol shown. Can you find any information on the security of the connection?

1.b Open Example2.pcap in Wireshark.

- Can you identify the domain name of the server? It might be somewhere within the packet.
- Which protocoals are used on application layer?
- Now open Chrome and type in the address that you have identified, using the protocol shown. Can you find any information on the security of the connection?

1.c Open Example3.pcap in Wireshark.

- Can you identify the domain name of the server?
- What is different to the other two examples?
- Which protocols are used?
- Now open Chrome and type in the address that you have identified, using the protocol shown. Can you find any information on the security of the connection?

Task 2: Certificates for HTTPS/TLS

2.a Use Chrome to open a webpage that supports TLS. For example https://combank.com.au/ Click on the lock shown on the left from the address bar.

- Who is the issuer of the certificate and how long is it valid?
- Which cipher suite is used?

2.b Can you find the list of all certification authorities that are installed in Chrome? Can you find some revoked certificates? (Hint: Look in settings under advanced settings)

3.b Now try another site that should be secure. It is the Australian Government website: https://www.australia.gov.au/
What happens? Does it work? If not, click on advanced to get some explanation. Click on the lock to see if the connection is encrypted and have a look at the certificate.