FIT2093 Tutorial 9

Topics

- TLS, HTTP, HTTPS
- Certificates for HTTPS
- Issues with HTTPS websites

Review

1. What is the place of TLS in the TCP/IP network stack?
2. What are the tasks of the TLS handshake and the TLS record protocol?
3. Explain why a VPN does not provide end-to-end encryption.
4. Why is it necessary that firewall filtering rules consider the destination port?
5. What is contradiction between filtering traffic by a firewall and encryption?

Task 1: TLS, HTTP, HTTPS

For this task you need to use *Wireshark* 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?
- Can you get information on the location of destination and source?
- 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?
- Identify which version of the security protocol is used. Is this considered to be a secure version?
- 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? Are these considered t0 be secure?
- 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?
- What is used for key exchange and which cipher suite is used during transport?

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)

2.c This article shows a few of the main issues with certificates: https://arstechnica.com/security/2017/03/google-takes-symantec-to-the-woodshed-for-mis-issuing-30000-https-certs/

(a) Read the article.

(b) What are the different entities (companies, software, etc.) that need to be trusted to actually trust a certificate?

(c) Draw a diagram showing the process of certificate issueing and checking in the browser. It should contain entities (companies, devices, software) used for producing the different certificates and checking it. Assume that the server's certificate is directly signed with the issuer's root certificate.

Task 3: HTTPS with correct certificate and no lock

Now, using Google Chrome, try two other sites that should be secure:

3.a First, the website of the Australian Government: https://www.australia.gov.au/
What happens? Does it work? Lets try http://www.australia.gov.au/

3.b Second, the website of the German Parliament (Bundestag): https://www.bundestag.de/en/
Does this work? can you see the lock showing a secure connection?
Id not, try to find out what happens. Is the certificate not valid? Is the certification authority untrusted? What else?