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?
- 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?
- Note that the server has been changed and the protocol is different to the one in the recorded Wireshark file.
- Does the location of the organisation match with the location of the server?

- The wireshark file just shows an extract with HTTP messages. Students should look at the different layers and see what kind of information they can get.
- The address is http://www.diamondbank.com/ This page used HTTP. No authenticity, no encryption. Location for the server in the US and Monash University can be found.
- Diamondbank is a bank from Nigeria, but the server is in Phoenix, AZ in the U.S. This can be seen in the GeoIP information shown in some Wireshark instances. On Windows, GeoIP information might not be shown.
- For security, you need to press Ctrl-Shift-i in Chrome to open the inspection window and then click ont he security tab.
- By now, Diamond bank has changed its Website. It now automatically refers to TLS. In Google Chrome, there should be the information that the connection is secure.

1.b Open Example2.pcap in Wireshark.

- Can you identify the domain name of the server? It might be somewhere within the packet.

- 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? Can you identify which encryption algorithms are used.

- The server is the one you get to when clicking on login on the 1.a website.
- https://diamondonline.diamondbank.com/
- It uses TLS. You will find, that the application layer protocol is http. However, you only find encrypted content.
- If you inspect the page in Chrome you will now find in the information on the security of the site that it uses TLS 1.2.
- Key exchange is ECDHE RSA and Cipher for encryption is AES 128 GCM.

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?

This time it is another server, but also using HTTP: http://combank.com.au. However, you will first see an error and then see that the get request was diverted to HTTPS. Thus, the traffic automatically switches from HTTP to TLSv1.2.

Task 2: Certificates for HTTPS/TLS

2.a Use Chrome to open a webpage that supports TLS. For example https://commbank.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? You might need to reload the page to see connection information.

DigiCert has issued the certificate. Expires on 27.02.2019.

TLS 1.2

Key Exchange: ECDHE RSA

This is Elliptic Curve Diffie-HEllman, signed with RSA.

Cipher Suite: AES 256 GCM

This is 256 bit AES used in Galois/Counter Mode.

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)

Just look in the menu -> settings -> advanced settings and scroll down to HTTPS/SSL and Manage certificates. Under servers, you find a few untrusted certificates. If someone is interested in the story behind this, google for UTN-USERFirst-Hardware.

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

(a) First, the website of the Commonwealth: https://www.commonwealthofnations.org/
What happens? Does it work? Lets try http://www.commonwealthofnations.org/

(b) Second, try a secure website and see if we can still change it.
Open https://www.pm.gov.au/
Is this page shown to the secure?
Can you make yourself prime minister so that the page still looks secure?
Hint: Right-click on the Name of the Prime Minister.
Why is it still shown as secure? Can this be a problem?

(a) Just wonder why the Commonwealth is not able to just get a certificate . . .

(b) If you inspect the code, in can also be changed and the changed version is shown.
This is only local and disappears on reload.
It is possible, because security (TLS) is between transport and application. This means, that the changes on application layer are not detected.
The problem is, that malware on the computer can do the same changes.