Transport Layer Security (TLS)

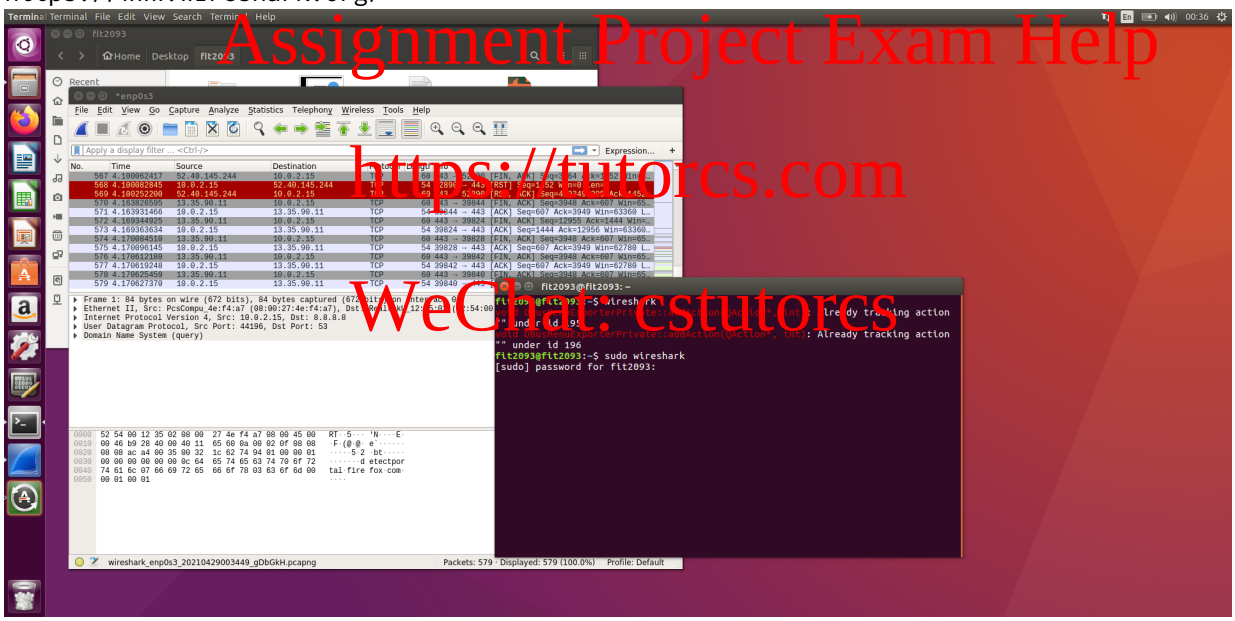
IMPORTANT NOTES:
Study lecture materials at least 1 hour and prepare Lab Task 3.1 prior to the lab session. Prepared questions will be discussed in the lab session.

1 Overview

The learning objective of this lab is for students to get familiar with TLS protocol.

2 Lab Environment

In this lab, we will use wireshark preinstalled in the cloud VM to analyse three captured packets files. Click "Applications–>Internet–>Wireshark" from the desktop to start the Wireshark. Alternatively, click any captured file in folder `/srv/fit2093files/fit2093lab/` such as `Example1.pcap` to open Wireshark. You may also choose to download and install the Wireshark on your own devices. More information can be found from `https://www.wireshark.org/`



3 Lab Tasks

3.1 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.

1. Start Wireshark and open `/srv/fit2093files/fit2093lab/Example1.pcap`.
   (a) Can you identify the domain name of the server?
   (b) Which protocols are used on application layer?

(c) Can you get information on the location of destination and source?

2. Open `/srv/fit2093files/fit2093lab/Example2.pcap` in Wireshark.

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

   (b) Which protocols are used on application layer?

   (c) Identify which version of the security protocol is used. Is this considered to be a secure version?

   (d) Find the `Client Hello` packet sent from client. What cryptographic functions are supported by the client?

   (e) Find the `Server Hello` packet sent from server in response. What `Cipher Suite` the server agrees to use?

   (f) What is the purpose of the `Change Cipher Spec`?

3. Open `/srv/fit2093files/fit2093lab/Example3.pcap` in Wireshark.

   (a) Can you identify the domain name of the server?

   (b) What is different to the other two examples?

   (c) Which protocols are used? Are these considered to be secure?

   (d) Compare the supported client `Cipher Suite` in `Client Hello` in `Example3.pcap` with the supported `Cipher Suite` in `Client Hello` in `Example2.pcap`. What is different?

   (e) What `Cipher Suite` the server agrees to use?

   (f) Using the RFC document for TLSv1.2 (RFC5246) explain what cryptographic algorithms are used in the agreed `Cipher Suite`.

3.2 Certificates for HTTPS/TLS

1. Use a web browser on your **own device** (**not** in the VM) 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.

   (a) Who is the issuer of the certificate and how long is it valid?

   (b) What is used for key exchange and which cipher suite is used during transport?

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

3. This article shows a few of the main issues with certificates:

   `https://arstechnica.com/information-technology/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 issuing 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.

3.3 Additional Task: Packet Capturing

Use Wireshark and try to capture the HTTPS haneshake messages on your own devices.