

Information Security, Spring, 2020  
Department of Information Management and Finance  
National Chiao Tung University

## Assignment 2

本次作業目標在於熟悉 SSL/TLS/HTTPS 的實際運作情形. 具體來說, 會請你側錄 SSL/TLS/HTTPS 的 traffic 然後用 sniffer (如 wireshark) 打開, 再請你指認出哪邊是 TLS handshake 的地方.

### 詳細說明

**Task 1.** Sniffer 是指可以監聽並側錄網路通訊的軟硬體, 目前最廣為人知的應該是 wireshark 這套軟體. 換言之, 如果安裝 wireshark 之後, 至少你可以監聽並側錄你自己電腦的網路通訊; 而錄下的 network traffic 被叫做 packet trace. 第一個任務是請你先安裝 sniffer (推薦但不強制使用 wireshark). 如果不熟析 wireshark 的同學可以在 Youtube 上找到多個 online tutorial 可以學習.

**Task 2.** 請隨機前往一個支援 HTTPS 的網頁, 並且側錄「瀏覽網頁」的 traffic (正式名稱是 packet trace). 這個步驟可以先把 wireshark 打開之後再前往該網頁, 並且目前 browser 有太多額外的功能, 因此也許可以試試看用 wget 這樣的 command line tool 來進行「瀏覽網頁」以求獲得比較乾淨的 packet trace.

**Task 3.** 從你的 packet trace 當中利用多個 screenshot 貼在報告裡面告訴我哪段時間是 TLS handshake, 並且哪些時候是 TLS handshake 的哪幾個步驟. 譬如下圖就是一個例子; 裡面可以指認出 Client Hello, Server Hello 等 TLS handshake 的步驟. 除此之外, 也需要針對每個步驟的細項參數解釋到底是何用意. 譬如下圖也是同樣一個例子; 裡面你可以解釋的是這是 TLS 1.0 的 handshake, Random 是 5017 開頭的 string, 這你需要解釋 Random 又是什麼意思拿來做什麼的等等. 這些細項的解釋請寫在報告內.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.021328	192.168.1.102	173.194.79.106	TLSv1	186	Client Hello
6	0.041634	173.194.79.106	192.168.1.102	TLSv1	1484	Server Hello
7	0.041697	173.194.79.106	192.168.1.102	TLSv1	377	Certificate, Server Hello Done

  

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 85

▼ Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 81

Version: TLS 1.0 (0x0301)

▼ Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f1376...

GMT Unix Time: Jul 31, 2012 07:18:59.000000000 GMT Daylight Time

Random Bytes: d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e0...

Session ID Length: 32

Session ID: 8530bdac95116ccb343798b36cb2fd79c1e278cba1af4145...

**Task 4.** 請撰寫報告 (可以接受 Word 與 Latex) 搭配 screenshot 與 packet trace 解說.

甚麼該出現在你的 report 裡?

- ✧ 你的 report 該出現你如何安裝 sniffer, 如何抓取 packet trace, 並且針對你的 packet trace 內的 TLS handshake 盡量做逐個細項的解釋.

該怎麼繳交 (若不符合規定則恕不接受)?

- ✧ Code 與報告一同壓縮後, 上傳至 e3 系統
- ✧ 繳交截止日 2020 年 6 月 3 日 23:59:59. 可以遲交一個禮拜, 但扣 20% 分數.