FIT1047 Applied Session Week 11

NETWORK SECURITY

OBJECTIVES

- The purpose of this applied session is getting to know (i) Transport Layer Security (TLS), HTTP and HTTPS (ii) Certificates for HTTPS.

INSTRUCTIONS

- For some of the questions, you may have to refer to the pre-class video and associated slides available in the Moodle.
- You may work in a small group.

Activity 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 web server.

Before you start, get Wireshark capture files *FIT1047-Applied-W11Q1a.pcap*, *FIT1047-Applied-W11Q1b.pcap* and *FIT1047-Applied-W11Q1c.pcap* from Moodle.

(a) Start Wireshark and open "FIT1047-Applied-W11Q1a.pcap".

i. Can you identify the domain name of the server?
ii. Which protocols are used on the application layer?
iii. Can you get information on the location of the destination? [Use IP address to find out location using any Geo-IP Locator, e.g. http://geoiplookup.net/]
iv. 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?

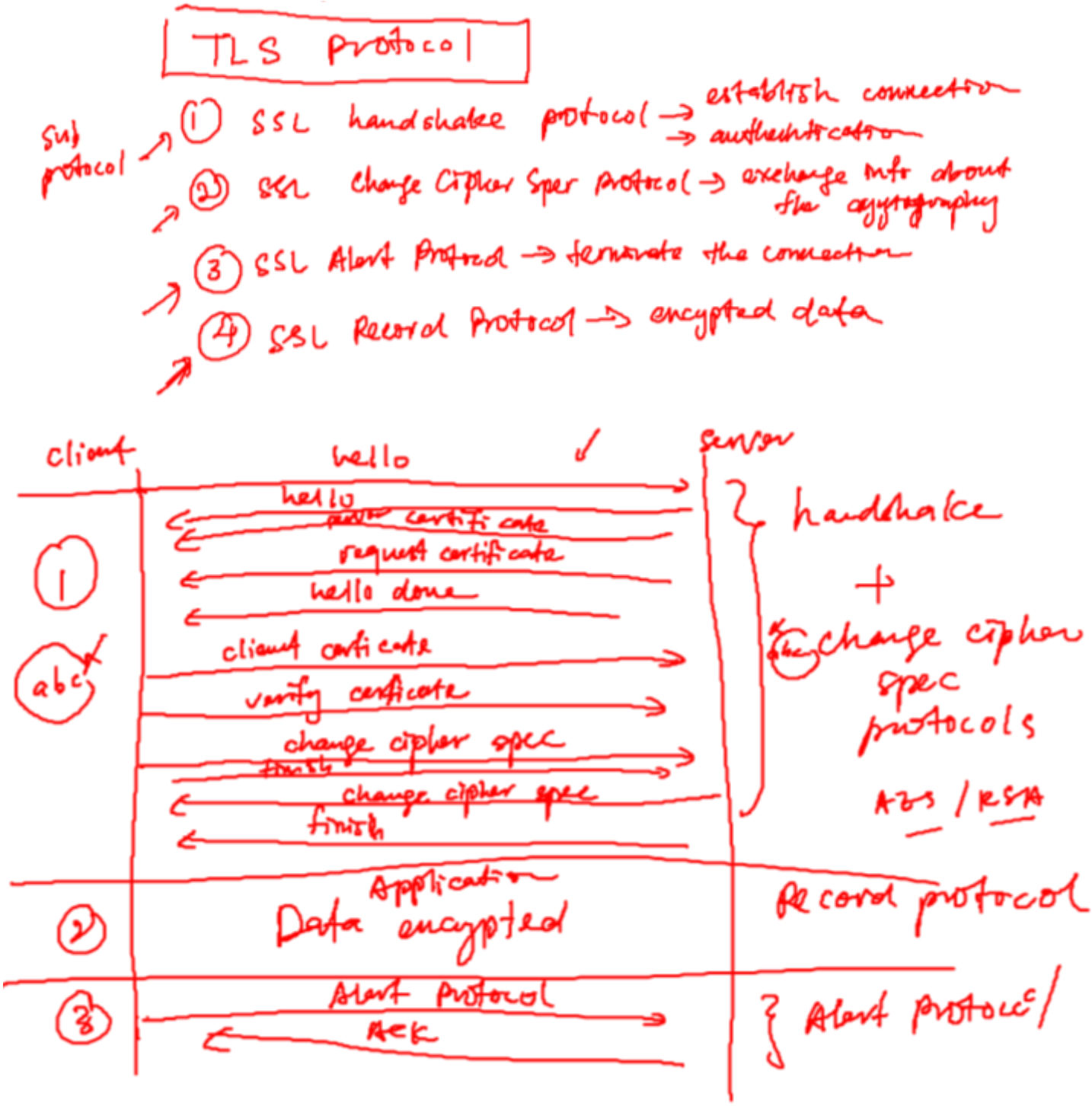
(b) Open "FIT1047-Applied-W11Q1b.pcap" in Wireshark.

i. Can you identify the domain name of the server? It might be somewhere within a packet.
ii. Which protocols are used on the application layer?
iii. 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?
iv. Can you identify which encryption algorithms are used?

(c) Open "FIT1047-Applied-W11Q1c.pcap" in Wireshark.

i. Can you identify the domain name of the server?
ii. Observing the change of protocol used in the sequence of packet exchange. What is different from the other two examples?
iii. Which protocols are used?

iv. 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?



Sample Solution:

(a) The wireshark file shows an extract of packet exchanges. We need to look at different layers and see what kind of information we can get.

i. The domain name: www.bom.gov.au
ii. Protocol used in Application Layer: HTTP.
iii. Location for the destination server: Melbourne, Australia
iv. Not Secure. Hence no encryption applied on the packets exchanged. In Google Chrome, there should be information that the connection is not secure. You need to press Ctrl-Shift-i in Chrome to open the inspection window and then click on the security tab.

(b) The wireshark file shows an extract of packet exchanges. We need to look at different layers and see what kind of information we can get.

i. The domain name: https://www.diamond.bank [Note: Inspect Frame 4-> Client Hello -> TLS -> Handshake Protocol -> server_name]
ii. It uses TLS. You will find that the application layer protocol “HTTP” is encrypted by TLS. You only find encrypted content.
iii. 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.
iv. This connection is completely secure. Identity of server is verified.

(c) The wireshark file shows an extract of packet exchanges. We need to look at different layers and see what kind of information we can get.

i. The domain name: http://combank.com.au.
ii. It starts the communication process using HTTP, then it switches to TLS. You will find that the application layer protocol changes from HTTP to TLSv1.2.
iii. First HTTP, then HTTPS
iv. It uses the EDHE_RSA key exchange method (Elliptic Curve Diffie-HEllman, signed with RSA). Encryption is performed using AES_256_GCM (256 bit AES used in Galois/Counter Mode)

Activity 2: Certificates for HTTPS/TLS

(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.

i. Who is the issuer of the certificate and how long is it valid?
ii. Which cipher suite is used? You might need to reload the page to see connection information.

(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)

(c) Now, using Google Chrome, try a secure website and see if we can still change it. Open the page at "https://www.pm.gov.au/"

i. Is this page shown to be secure?
ii. Can you make yourself prime minister so that the page still looks secure? Hint: Right-click on the Name of the Prime Minister.
iii. Why is it still shown as secure? Can this be a problem?

Sample Solution:

(a) Answers:

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.

(b) Answers:

Just look in the menu -> settings -> advanced settings and scroll down to HTTPS/SSL and Manage certificates. Under servers, you may find a few untrusted certificates.

(c) Answers:

It is secure. If you inspect the code, it can also be changed and the changed version is shown in the local display. This is only local and disappears on reload.

Activity 3: Diffie-Hellman key exchange

Alice (a) and Bob (b) wish to do Diffie-Hellman key exchange. Alice and Bob have agreed upon a prime p = 47, and a generator g = 5. Alice has chosen her private exponent to be: a = 3, while Bob has chosen his private exponent to be b =7.

Calculate the shared secret key. Show all intermediate steps.

1. Alice and Bob agree on base g and modulus p (g needs to be a primitive root modulo p), g and p are public. Example: g=5 and p=47

2a. **Alice choses** (random) secret **a** and computes **$A=g^a \bmod p$**

Example: a=3, then $A=5^3 \bmod 47 = 125 \bmod 47 = 31$

2b. **Bob choses** (random) secret **b** and computes **$B=g^b \bmod p$**

Example: b=7, then $B=5^7 \bmod 47 = 78125 \bmod 47 = 11$

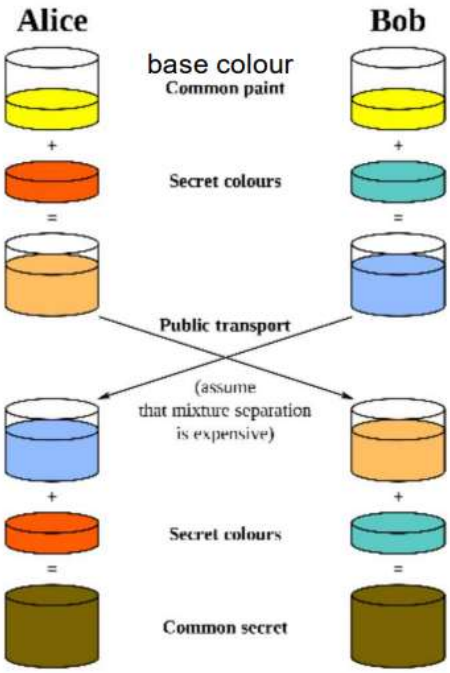
3. They **exchange A=31 and B=11**

4.Shared key is $K=B^a \bmod p = g^{ba} \bmod p = g^{ab} \bmod p = A^b \bmod p$

A calculates B^a mod n = 11^3 mod 47 = 1331 mod 47 = **15**

B calculates A^b mod n = 31^7 mod 47 = 27512614111 mod 47 = **15**

Diffie-Hellman, Paint Analogy



	Alice	Evil Eve	Bob
	Alice and Bob exchange a large Prime integer (q=11) and a primitive root (a=7) a=7, q=11	Evil Eve sees q=11, a=7. This needs to be exchanged in secure way !	Alice and Bob exchange a large Prime integer (q=11) and a primitive root (a=7) a=7, q=11
Step: 1	Alice generates a random number (Private_Key): X_A such that $X_A < q$ $X_A = 6$ (Secret)		Bob generates a random number (Private_Key): X_B such that $X_B < q$ $X_B = 9$ (Secret)
Step: 2	compute their public key: y_A $y_A = a^{XA} \bmod q$ $y_A = 7^6 \pmod{11}$ $y_A = 4$		compute their public key: y_B $y_B = a^{XB} \bmod q$ $y_A = 7^9 \pmod{11}$ $y_B = 8$
Step: 3	Alice receives $Y_B = 8$ in clear-text	Evil Eve sees $Y_A = 4$, $Y_B = 8$	Bob receives $Y_A = 4$ in clear-text
Step: 4	Secret Key = $K_{AB} = y_B^{XA} \bmod q$ (which Alice can compute) Secret Key = $8^6 \pmod{11}$ Secret Key = 3		Secret Key = $K_{AB} = y_A^{XB} \bmod q$ (which Bob can compute) Secret Key = $4^9 \pmod{11}$ Secret Key = 3