Wireless Trace analysis

Due date:

In this assignment, you will be analyzing packet traces using the Wireshark software tool. In this homework, two packet traces are provided and can be downloaded from Avenue. The two packet traces correspond to frames exchanged between a mobile device and wireless access points. In the first trace, the device connects to MacSecure, a secure WLAN; and in the second trace, the device connects to MacConnect, an open WLAN. The MAC address of the mobile device is 18:34:51:18:AF:01 (Apple_18:af:01).

MacSecure trace: Open the file MacSecure.pcap in Wireshare (using "File" $\rightarrow$ "Open"). You will see a split screen with the top half showing the frames captured over time, and the bottom half showing the information of the highlighted frame in the top half. One can click the arrows on the left to expand for further information. Answer the following questions:

1) Can you guess what is the vendor (manufacture) of the APs for MacSecure?
2) What is the type of the first frame (at time 0.0)? Why is the SSID set to "Broadcast"?
3) What are the types of the frames numbered 2, 3, 4? What information is contained in the Radiotap header, and the IEEE 802.11 wireless LAN management frame?
4) Explain the frames 29 and 30.
5) Which channel does the AP operate that the mobile is associated with?
6) Between frame 31 - 44, how many association requests have been sent from the mobile device
7) Which extended authentication protocol(s) (EAP) is used by MacSecure (e.g., EAP-TTLS/MSCHAPv2, EAP-TTLS, etc.)
8) Which EAP is used in authenticating the mobile device?
9) Frame 71 indicates the success of authentication via 802.11X. Which frames correspond to the 4-way handshake for establishing pair-wise transient key? What are the nonces used by the AP and the mobile devices in the 4-way exchange?
10) Why cannot we see DHCP message exchanges in the trace for address allocation?

MacConnect trace: MacConnect provides unencrypted open access to campus WiFi. It uses web login to authenticate users.

1) Type "Bootp" in the filter field to display only DHCP related messages. A DHCP NAK message by the DHCP server is sent when a requested address is not available. From DHCP request message 77 - 101, what is the requested address by the mobile? What is the IP address allocated to the mobile eventually?
2) What is the purpose of the gratuitous ARP in frame 136?
3) Type "SSL" (or "ssl") in the filter field to display SSL messages that are used to authenticate the user. From the frame 243 - 273, identify the type of messages exchanged and the values of the angle bracket (<>) in reference to Figure 1 that describes the connection setup process in SSL.

Submission: Whenever possible, when answering a question, you should include a screenshot of the information of the packet(s) within the trace that you used to answer the question asked. Highlight relevant areas (e.g, using circles, arrows) of the screenshots to explain your answer. Include your answers and screen shots if any in a single PDF file named YOUR_MAC_ID_A6.pdf. Submission should be done through Avenue.

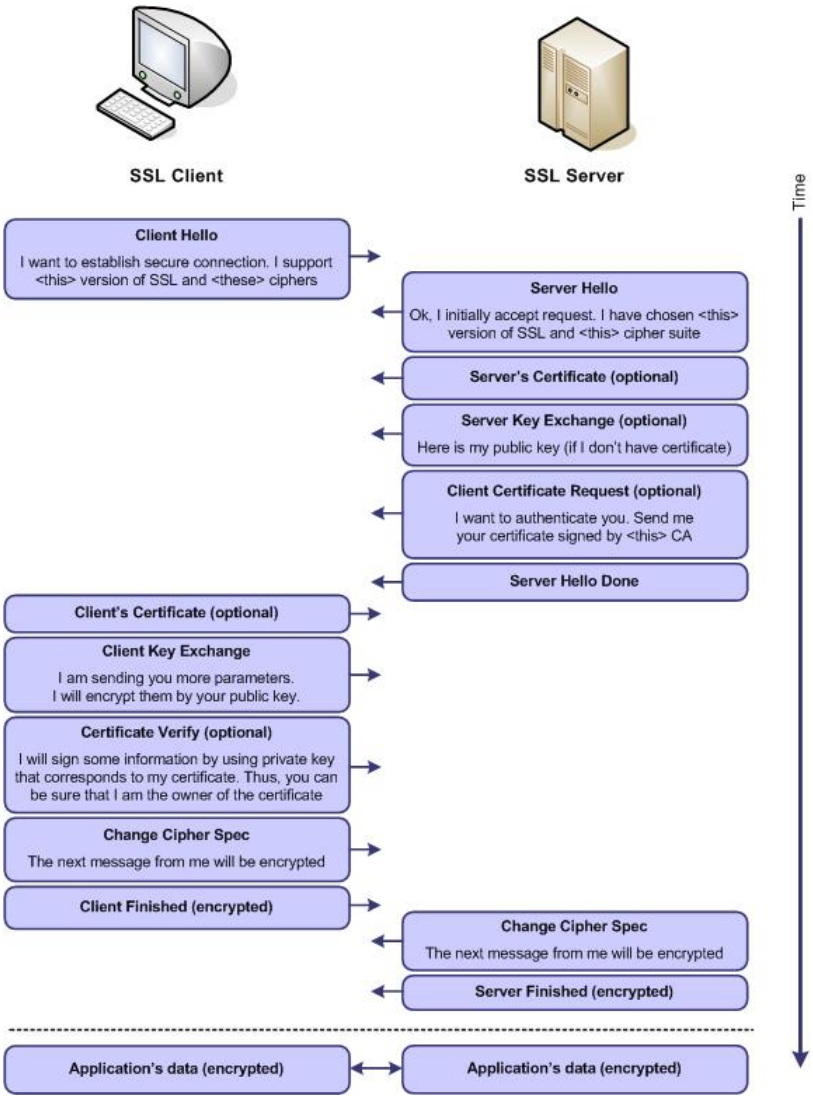

Fig. 1. SSL connection setup