COSC 450 Assignment 3 Fall 20

Upload the three files groupnamea3cap, groupnamea3tls and groupnamea3wifi to Blackboard.

1. Start Wireshark and capture packets. Use the Mozilla Firefox browser to send a request to: https://eecs.berkeley.edu/ Capture all the packets sent and received due to the above request. Stop the capture to minimize the number of packets captured. Save the capture in a file groupnamea3cap. Check that Wireshark can open the saved .pcapng file and display the packets. Use the captured packets to give brief answers to the questions below. For each answer, indicate the relevant Wireshark frame numbers for the packets you are using in your answers. Put your answers in a file groupnamea3tls.

1.1 List the Wireshark names for all the TLS handshake messages (between the above server and the browser) such as Client Hello, Server Hello and ending with the Change Cipher Spec and EncryptedHandshakeMessage from the server.
Client Hello – Frames 107
Server Hello – Frame 109
Key Exchange – 112
Change Cipher Spec – 117

1.2 What is the string sent by the server to indicate the chosen cipher suite? What algorithms are in this string and what is the purpose of each algorithm? The handshake certificate will indicate the chosen cipher suite with an algorithm of SHA256 with RSA Encryption

1.3 What are the organization names in the certificates sent by the server? How does the browser use these certificates?
Cs.berkeley.edu. The browser uses this to encrypt its own certificate to the server.

1.4 In the Server Key Exchange Message, what are the lengths in bytes of the public key and the signature? What type of public key is sent in this message and in the Client Key Exchange message? Refer to RFC 8422 Sections 2.1 and 2.2, and briefly explain how TLS premaster secret is computed by using the server's and client's public keys that are exchanged in these messages.
The length is 296 bytes, and the type of key is a EC Diffie-Hellman key. The same type of key is sent to the client key exchange just of different length. During the TLS premaster secret is generated by the client sending a random string of bytes. The secret is encrypted with the public key, and can only be decrypted by the private key of the server.

1.5 Consider the Wireshark frame F that is labelled as containing Certificate, Certificate Status and Server Key Exchange. According to Wireshark, what is the TCP payload length and what is the TCP segment length in this frame F? Explain why these two lengths are not the same. These two lengths are given in bytes below the information labeled as [Timestamps].
Payload length is 900 bytes, TCP Segment length is 46 bytes. This is to help protect the integrity of the data in the segment. As such the payload is used in the authentication and the segment is the actual data supposably.

2. Go to: https://drive.google.com/drive/folders/0B4-AWwD5siI1VFVTU01aV3QxWHc
Download the file: wirelesseapolfiltered.pcap and open it using Wireshark.
The EAP frames of interest are labeled by Wireshark as:
802.1X Authentication/Extensible Authentication Protocol (where the EAP fields are Code, Id, Length and Type) or as 802.1X Authentication/EAPOL. Use these frames to answer the questions below and put your answers in a file groupnamea3wifi.

2.1 What is the frame number for the EAP frame that the client uses to request EAP-TLS? What is the EAP field Type for this frame and what TLS flags are set in this frame?
Frame 32, Type: TLS EAP (EAP-TLS) (13), Flags are 0x20

2.2 What is the frame number for the EAP frame that has the Client Hello? What is the EAP field Type for this frame and what TLS flags are set in this frame?
Frame 38, Tpye Protected EAP (EAP-PEAP) (25), Flags: 0x01

2.3 What is the frame number for the EAP Success frame? What field in this frame indicates that it is the EAP Success frame and what is the numeric value of this field?
Frame 78 EAP Field with an ID of 45

2.4 The four frames of the 4-way handshake are EAPOL frames. What are the frame numbers for these four frames? These frames contain values (possibly 0) for the fields Nonce, MIC, Key Data and Replay Counter. Briefly discuss the purpose of including these values in <u>each</u> of the four frames.

Frames: 80 82 85 87

The 4 fields are used in the 4-way handshake. Between the access point, client device so that they can generate some encryption keys to be used to encrypted data over a wireless connection.