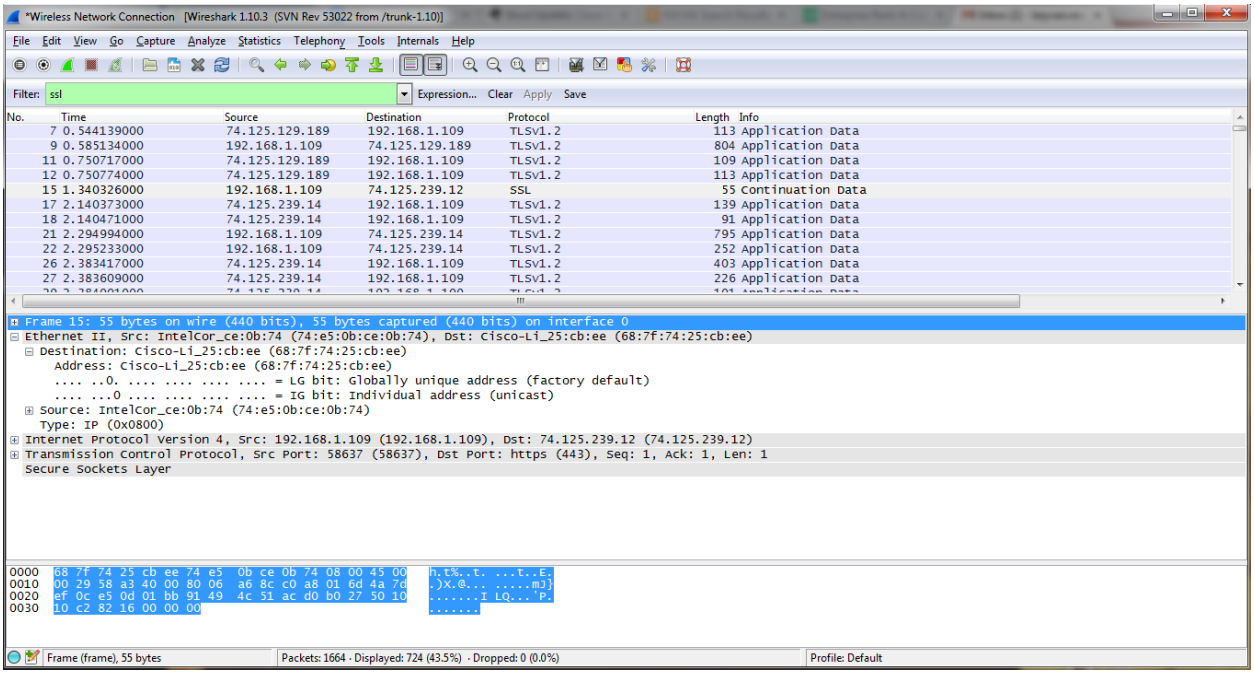
Solutions to Lab4

EE 450

Dr. Walker

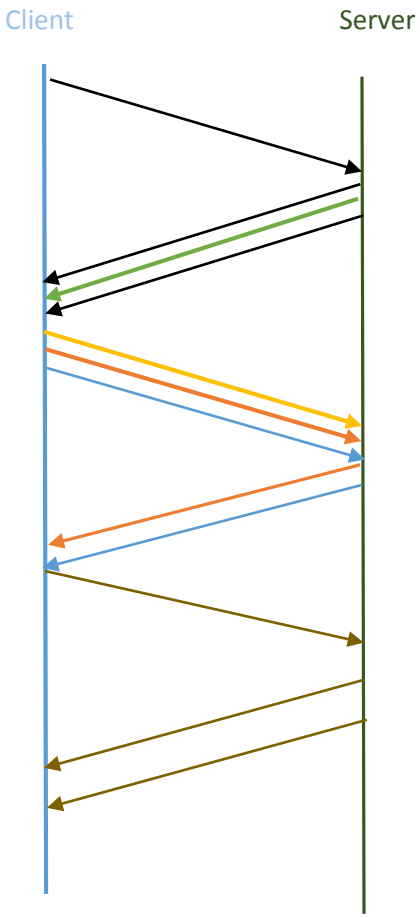
One screen shot of my wireshark lab filtering the SSL packets:



1) The source 6 of the packets is my own laptop and their destination is a cisco server. The other two are replies from the cisco webservers to my laptop:
   The first six packet Source: 192.168.1.109
   The next two packet Source: 205.251.242.54

The other information about them is as follows:

Pkt No	Frame No	# SSL Records	SSL Record Type	Source of the Frame	Frame Info
1	1	1	Hand shake	Client	Client Hello
2	68	1	Hand shake	Server	Server Hello
3	71	2	Hand shake	Server	Certificate
4	73	3	Hand shake, Change Cipher, Hand shake	Client	Key exchange, change cypher, encrypted hand shake
5	79	2	Change Cipher, Hand shake	Server	
6	82	1	Data	Client	
7	93	1	Data	Server	
8	99	1	Data	Server	



2) You can find these three filed under the section of Secure Socket Layer. By clicking on each you will see the corresponded bytes highlighted.

Content Type	1byte
Version	2byte
Length	2byte

3) content type: Handshake (22)
Handshake type: Client Hello (1)

4) There is no 'nonce' or 'challenge' field in the Client Hello record. However there is a 'random' field which serves the same purpose as 'nonce' in TLSv1.0 Value of this is:
4bed64f0f5e4485bc80e05c52c167d6d82265dce9e336ba97944b729

5) Yes.

Public key algorithm	ECDSA (Elliptic curve cryptography)
Symmetric key algorithm	AES
Hash key algorithm	SHA

6) The server suite uses TLS_RSA_WITH_RC4_128_SHA that is:

Public key algo:	RSA
Symmetric key algo:	RC4
Hash key algo:	SHA

7) This contains a random field which has a random number generated by server, 28 bytes long. The purpose of nonces in SSL is to prevent a replay attack, which is prevented by concatenating password with random number from server and then sending the hash of it.

8) Yes this record includes a session ID. It provides a unique identifier for the SSL session. The client may resume the same session later by using this server provided session ID when it sends the ClientHello.

9) There is no certificate, in this record. It is in another record for certificate. It does fit into a single Ethernet frame.

10) Yes, this record does contain a pre-master secret. It is used by the server and client to make a master secret, which is used to generate session keys for MAC and encryption. Yes the secret is encrypted, using RSA (since it was chosen by the server, evident in server hello) and is 256 bytes long.

11) The change cipher spec record indicates that the contents of the following SSL records will be encrypted. Change cipher spec record is 6 bytes long.

Content type:	1 byte
Version:	2 bytes
Length:	2 bytes
Change Cipher spec message:	1 byte

12) All previous handshake messages sent from client are encrypted. It is done by MAC of the concatenation of all the previous handshake messages sent from the client is generated and sent to the server.

13) Yes the server also sends a Change Cipher Spec record and Encrypted Handshake to the client. It is different as it contains the concatenation of all the handshake messages sent from the server rather than from the client.

14) The application data is encrypted using the symmetric key algorithm in cipher suite specifications as was agreed upon by client and server earlier during client and server hello and the pre-master secret key and nonces obtained from client and server. The client encryption key is used to encrypt data from client to server and server encryption key to encrypt data from server to client. Yes application data does contain a MAC and the data+Mac is encrypted in each record. No, wire shark cannot distinguish between encrypted application data and a MAC.

15) In higher versions of TLS, a clever use of random bytes is made as a nonce. The random bytes being generated at client and server separately will ensure high probability of uniqueness and thereby prevent replay attacks more effectively.