

HO CHI MINH UNIVERSITY OF TECHNOLOGY
Faculty of Computer Science and Engineering



Computer Networks

Report for lab 8

Lecturer: Nguyễn Mạnh Thìn
Student name: Đặng Trần Khánh-1852037



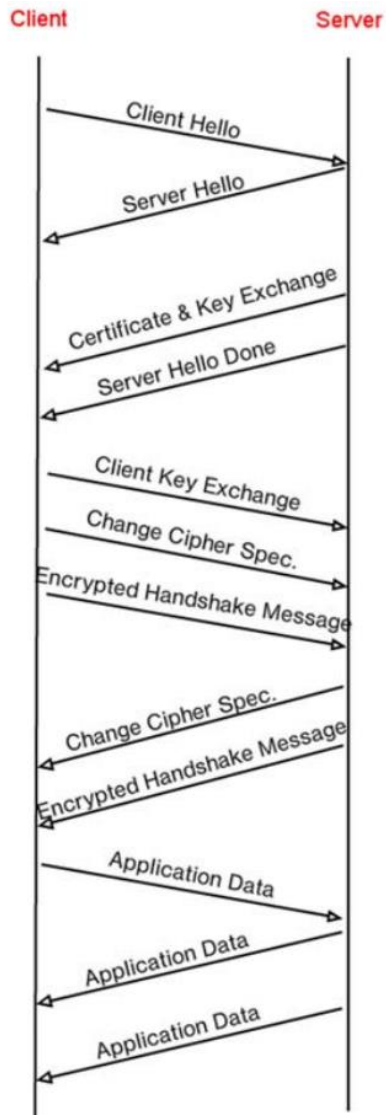
1/ For each of the first 8 Ethernet frames, specify the source of the frame (client or server), determine the number of SSL records that are included in the frame, and list the SSL record types that are included in the frame. Draw a timing diagram between client and server, with one arrow for each SSL record?

Answer:

No.	Time	Source	Destination	Protocol	Length	Info
106	21.885705	128.238.38.162	216.75.194.220	SSLv2	132	Client Hello
108	21.830201	216.75.194.220	128.238.38.162	SSLv3	1434	Server Hello
111	21.853520	216.75.194.220	128.238.38.162	SSLv3	790	Certificate, Server Hello Done
112	21.876168	128.238.38.162	216.75.194.220	SSLv3	258	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
113	21.945667	216.75.194.220	128.238.38.162	SSLv3	121	Change Cipher Spec, Encrypted Handshake Message
114	21.954189	128.238.38.162	216.75.194.220	SSLv3	806	Application Data
122	23.480352	216.75.194.220	128.238.38.162	SSLv3	272	Application Data
149	23.559497	216.75.194.220	128.238.38.162	SSLv3	1367	Application Data
158	23.560866	216.75.194.220	128.238.38.162	SSLv3	1367	Application Data
163	23.566451	128.238.38.162	216.75.194.220	SSLv3	156	Client Hello
165	23.586650	216.75.194.220	128.238.38.162	SSLv3	1329	Application Data

No	Frame	Source	Destination	SSL count	SSL Type
1	106	128.238.38.162	216.75.194.220	1	Client Hello
2	108	216.75.194.220	128.238.38.162	1	Server Hello
3	111	216.75.194.220	128.238.38.162	2	Server Hello Done
4	112	128.238.38.162	216.75.194.220	3	Client Key Exchange
5	113	216.75.194.220	128.238.38.162	2	Change Cipher Spec
6	114	128.238.38.162	216.75.194.220	1	Application Data
7	122	216.75.194.220	128.238.38.162	1	Application Data
8	149	216.75.194.220	128.238.38.162	1	Application Data

Timing diagram:



2/Each of the SSL records begins with the same three fields (with possibly different values). One of these fields is “content type” and has length of one byte. List all three fields and their lengths.

Answer: Content Type = 1 byte

Version = 2 bytes

Length = 2 bytes

```
> Frame 112: 258 bytes on wire (2064 bits), 258 bytes captured (2064 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.162, Dst: 216.75.194.220
> Transmission Control Protocol, Src Port: 2271, Dst Port: 443, Seq: 79, Ack: 2785, Len: 204
  Transport Layer Security
    SSLv3 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: SSL 3.0 (0x0300)
      Length: 132
      > Handshake Protocol: Client Key Exchange
    SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: SSL 3.0 (0x0300)
      Length: 1
      Change Cipher Spec Message
    SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: SSL 3.0 (0x0300)
```

0030	fd 1f c2 d9 00 00 16 03 00 00 84 10 00 00 80 bc-.....
0040	49 49 47 29 aa 25 90 47 7f d0 59 05 6a e7 89 56	II(G)·%·G ··Y·j··V
0050	c7 7b 12 af 08 b4 7c 60 9e 61 f1 04 b0 fb f8 3e	-{·-·-· ·~·a·-·-·>

3/Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?

Answer:

The content type is 22, for Handshake message type of 01, Client Hello.

106	21.805705	128.238.38.162	216.75.194.220	SSLv2	132 Client Hello
108	21.830201	216.75.194.220	128.238.38.162	SSLv3	1434 Server Hello
111	21.853520	216.75.194.220	128.238.38.162	SSLv3	790 Certificate, Server Hello Done
112	21.876168	128.238.38.162	216.75.194.220	SSLv3	258 Client Key Exchange, Change Cipl

> Transmission Control Protocol, Src Port: 2271, Dst Port: 443, Seq: 1, Ack: 1, Len: 78					
▼ Transport Layer Security					
▼ SSLv2 Record Layer: Client Hello					
[Version: SSL 2.0 (0x0002)]					
Length: 76					
Handshake Message Type: Client Hello (1)					
Version: SSL 3.0 (0x0300)					
Cipher Spec Length: 51					
Session ID Length: 0					
Challenge Length: 16					
▼ Cipher Specs (17 specs)					
Cipher Spec: TLS_RSA_WITH_RC4_128_MD5 (0x000004)					
Cipher Spec: TLS_RSA_WITH_RC4_128_SHA (0x000005)					
Cipher Spec: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x00000a)					
Cipher Spec: SSL2_RC4_128_WITH_MD5 (0x010080)					
Cipher Spec: SSL2_DES_192_EDE3_CBC_WITH_MD5 (0x0700c0)					
Cipher Spec: SSL2_RC2_128_CBC_WITH_MD5 (0x030080)					
Cipher Spec: TLS_RSA_WITH_DES_CBC_SHA (0x000009)					
Cipher Spec: SSL2_DES_64_CBC_WITH_MD5 (0x060040)					
Cipher Spec: TLS_RSA_EXPORT1024_WITH_RC4_56_SHA (0x000064)					
Cipher Spec: TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA (0x000062)					
Cipher Spec: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x000003)					
Cipher Spec: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x000006)					
Cipher Spec: SSL2_RC4_128_EXPORT40_WITH_MD5 (0x020080)					
Cipher Spec: SSL2_RC2_128_CBC_EXPORT40_WITH_MD5 (0x040080)					
Cipher Spec: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x000013)					
Cipher Spec: TLS_DHE_DSS_WITH_DES_CBC_SHA (0x000012)					
Cipher Spec: TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA (0x000063)					
Challenge					

0000	00 00 0c 07 ac 00 00 09	6b 10 60 99 08 00 45 00k-...E-
0010	00 76 48 28 40 00 80 06	6f a1 80 ee 26 a2 d8 4b	..vH(@...o...&..K
0020	c2 dc 08 df 01 bb 56 d2	08 c5 4c 9e 64 9f 50 18V-..L.d.P-
0030	ff ff e7 55 00 00 80 4c	01 03 00 00 33 00 00 00	...U...L....3...
0040	10 00 00 04 00 00 05 00	00 0a 01 00 80 07 00 c0
0050	03 00 80 00 00 09 06 00	40 00 00 64 00 00 62 00@..d..b-
0060	00 03 00 00 06 02 00 80	04 00 80 00 00 13 00 00
0070	12 00 00 63 66 df 78 4c	04 8c d6 04 35 dc 44 89	...cf-xL....5.D-
0080	89 46 99 09		..F..

4/Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

Answer: 66 df 78 4c 04 8c d6 04 35 dc 44 89 89 46 99 09

Cipher Spec: TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA (0x000012)			
Cipher Spec: TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA (0x000063)			
Challenge			

0010	00 76 48 28 40 00 80 06	6f a1 80 ee 26 a2 d8 4b	..vH(@...o...&..K
0020	c2 dc 08 df 01 bb 56 d2	08 c5 4c 9e 64 9f 50 18V-..L.d.P-
0030	ff ff e7 55 00 00 80 4c	01 03 00 00 33 00 00 00	...U...L....3...
0040	10 00 00 04 00 00 05 00	00 0a 01 00 80 07 00 c0
0050	03 00 80 00 00 09 06 00	40 00 00 64 00 00 62 00@..d..b-
0060	00 03 00 00 06 02 00 80	04 00 80 00 00 13 00 00
0070	12 00 00 63 66 df 78 4c	04 8c d6 04 35 dc 44 89	...cf-xL....5.D-
0080	89 46 99 09		..F..

5/ Does the ClientHello record advertise the cyber suites it supports? If so, in the first listed suite, what are the public-key algorithm, the symmetric-key algorithm, and the hash algorithm?

Answer:

Public key algorithm: RSA

Symmetric-key algorithm: RC4

Hash algorithm: MD5

No.	Time	Source	Destination	Protocol	Length	Info
106	21.805705	128.238.38.162	216.75.194.220	SSLv2	132	Client Hello
108	21.830201	216.75.194.220	128.238.38.162	SSLv3	1434	Server Hello
111	21.853520	216.75.194.220	128.238.38.162	SSLv3	790	Certificate, Server Hello D
112	21.876168	128.238.38.162	216.75.194.220	SSLv3	258	Client Key Exchange, Change

> Transmission Control Protocol, Src Port: 2271, Dst Port: 443, Seq: 1, Ack: 1, Len: 78
✓ Transport Layer Security

✓ SSLv2 Record Layer: Client Hello

[Version: SSL 2.0 (0x0002)]
Length: 76
Handshake Message Type: Client Hello (1)
Version: SSL 3.0 (0x0300)
Cipher Spec Length: 51
Session ID Length: 0
Challenge Length: 16

✓ Cipher Specs (17 specs)

Cipher Spec: TLS_RSA_WITH_RC4_128_MD5 (0x000004)
Cipher Spec: TLS_RSA_WITH_RC4_128_SHA (0x000005)
Cipher Spec: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x00000a)
Cipher Spec: SSL2_RC4_128_WITH_MD5 (0x010080)
Cipher Spec: SSL2_DES_192_EDE3_CBC_WITH_MD5 (0x0700c0)
Cipher Spec: SSL2_RC2_128_CBC_WITH_MD5 (0x030080)
Cipher Spec: TLS_RSA_WITH_DES_CBC_SHA (0x000009)
Cipher Spec: SSL2_DES_64_CBC_WITH_MD5 (0x060040)
Cipher Spec: TLS_RSA_EXPORT1024_WITH_RC4_56_SHA (0x000064)
Cipher Spec: TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA (0x000062)
Cipher Spec: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x000003)
Cipher Spec: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x000006)
Cipher Spec: SSL2_RC4_128_EXPORT40_WITH_MD5 (0x020080)
Cipher Spec: SSL2_RC2_128_CBC_EXPORT40_WITH_MD5 (0x040080)
Cipher Spec: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x000013)
Cipher Spec: TLS_DHE_DSS_WITH_DES_CBC_SHA (0x000012)
Cipher Spec: TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA (0x000063)
Challenge

6/Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?

Answer:

Public key algorithm: RSA

Symmetric-key algorithm: RC4

Hash algorithm: MD5

106	21.805705	128.238.38.162	216.75.194.220	SSLv2	132 Client Hello
108	21.830201	216.75.194.220	128.238.38.162	SSLv3	1434 Server Hello
111	21.853520	216.75.194.220	128.238.38.162	SSLv3	790 Certificate, Server Hello Don
112	21.876168	128.238.38.162	216.75.194.220	SSLv3	258 Client Key Exchange, Change C


```

> Frame 108: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits)
> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)
> Internet Protocol Version 4, Src: 216.75.194.220, Dst: 128.238.38.162
> Transmission Control Protocol, Src Port: 443, Dst Port: 2271, Seq: 1, Ack: 79, Len: 1380
v Transport Layer Security
  v SSLv3 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: SSL 3.0 (0x0300)
    Length: 74
  v Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 70
    Version: SSL 3.0 (0x0300)
  > Random: 0000000042dbed248b8831d04cc98c26e5badc4e267c3919...
    Session ID Length: 32
    Session ID: 1bad05faba02ea92c64c54be4547c32f3e3ca63d3a0c86dd...
    Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
    Compression Method: null (0)

```

7/ Does this record include a nonce? If so, how long is it? What is the purpose of the client and server nonces in SSL?

Answer: Yes, this package does include a nonce under Random field. It is 32 bits long (28bits data + 4 bits time), it is used for attack preventing.

Version: SSL 3.0 (0x0300)

Random: 0000000042dbed248b8831d04cc98c26e5badc4e267c3919...

GMT Unix Time: Jan 1, 1970 07:00:00.00000000 SE Asia Standard Time

Random Bytes: 42dbed248b8831d04cc98c26e5badc4e267c391944f0f070...

Session ID Length: 32

Session ID: 1bad05faba02ea92c64c54be4547c32f3e3ca63d3a0c86dd...

Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)

Compression Method: null (0)

0040	00 00 00 00 00 42 db ed 24 8b 88 31 d0 4c c9 8cB..\$.1.L..
0050	26 e5 ba dc 4e 26 7c 39 19 44 f0 f0 70 ec e5 77	&...N& 9.D..p..w
0060	45 20 1b ad 05 fa ba 02 ea 92 c6 4c 54 be 45 47	E.....LT.EG
0070	c3 2f 3e 3c a6 3d 3a 0c 86 dd ad 69 4b 45 68 2d	./><.=:..iKEh-
0080	a2 2f 00 04 00 16 03 00 0a 83 0b 00 0a 7f 00 0a	./.....

8/ Does this record include a session ID? What is the purpose of the session ID?

Answer: This record does include a session ID as described in the picture below. This session is for resume the same session later by using the server provided session ID when it sends the ClientHello.

108	21.830201	216.75.194.220	128.238.38.162	SSLv3	1434 Server Hello
111	21.853520	216.75.194.220	128.238.38.162	SSLv3	790 Certificate, Server Hello Done
112	21.876168	128.238.38.162	216.75.194.220	SSLv3	258 Client Key Exchange, Change Cipher

> Frame 108: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits)

> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)

> Internet Protocol Version 4, Src: 216.75.194.220, Dst: 128.238.38.162

> Transmission Control Protocol, Src Port: 443, Dst Port: 2271, Seq: 1, Ack: 79, Len: 1380

▼ Transport Layer Security

▼ SSLv3 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: SSL 3.0 (0x0300)

Length: 74

▼ Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 70

Version: SSL 3.0 (0x0300)

▼ Random: 0000000042dbed248b8831d04cc98c26e5badc4e267c3919...

GMT Unix Time: Jan 1, 1970 07:00:00.00000000 SE Asia Standard Time

Random Bytes: 42dbed248b8831d04cc98c26e5badc4e267c391944f0f070...

Session ID Length: 32

Session ID: 1bad05faba02ea92c64c54be4547c32f3e3ca63d3a0c86dd...

Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)

Compression Method: null (0)

9/ Does this record contain a certificate, or is the certificate included in a separate record. Does the certificate fit into a single Ethernet frame?

Answer: No, there is no certificate in this record. The certificate is in the separate record. The certificate does fit into a single Ethernet frame.

10/ Locate the client key exchange record. Does this record contain a pre-master secret? What is this secret used for? Is the secret encrypted? If so, how? How long is the encrypted secret?

Answer: Yes, it does contain a premaster secret. It is used by both the server and client to make a master secret, which is used to generate session keys for MAC and encryption. The secret gets encrypted using the server's public key, which the client extracted from the certificate sent by the server. The secret is 128 bytes long.

111	21.853520	216.75.194.220	128.238.38.162	SSLv3	790 Certificate, Server Hello Done
112	21.876168	128.238.38.162	216.75.194.220	SSLv3	258 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

> Frame 112: 258 bytes on wire (2064 bits), 258 bytes captured (2064 bits)

> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)

> Internet Protocol Version 4, Src: 128.238.38.162, Dst: 216.75.194.220

> Transmission Control Protocol, Src Port: 2271, Dst Port: 443, Seq: 79, Ack: 2785, Len: 204

▼ Transport Layer Security

 ▼ SSLv3 Record Layer: Handshake Protocol: Client Key Exchange

 Content Type: Handshake (22)

 Version: SSL 3.0 (0x0300)

 Length: 132

 ▼ Handshake Protocol: Client Key Exchange

 Handshake Type: Client Key Exchange (16)

 Length: 128

 ▼ RSA Encrypted PreMaster Secret

 Encrypted PreMaster: bc49494729aa2590477fd059056ae78956c77b12af08b47c...

 ▼ SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec

 Content Type: Change Cipher Spec (20)

 Version: SSL 3.0 (0x0300)

 Length: 1

 Change Cipher Spec Message

 ▼ SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message

 Content Type: Handshake (22)

 Version: SSL 3.0 (0x0300)

 Length: 56

 Handshake Protocol: Encrypted Handshake Message

11/ What is the purpose of the Change Cipher Spec record? How many bytes is the record in your trace?

Answer: The purpose of the Change Cipher Spec record is to indicate that the contents of the following SSL records sent by the client (data, not header) will be encrypted. This record is 6 bytes long: 5 for the header and 1 for the message segment.

SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec		
Content Type: Change Cipher Spec (20)		
Version: SSL 3.0 (0x0300)		
Length: 1		
Change Cipher Spec Message		
SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message		
Content Type: Handshake (22)		
Version: SSL 3.0 (0x0300)		
Length: 56		
Handshake Protocol: Encrypted Handshake Message		

0090	04 6e 5a 00 98 2e 52 ee b5 bc d1 c4 f5 63 f0 e3	.nZ...R.c..
00a0	44 29 f1 c6 ba 64 58 79 46 9e 3e c4 fd d7 9b 7a	D)...dXy F->....z
00b0	02 04 09 32 f6 1d 7a a1 2d cf d2 1a 18 64 29 14	...2...z.d).
00c0	03 00 00 01 01 16 03 00 00 38 29 a9 dc 11 5a 748)...Zt
00d0	7a 41 48 15 4f 50 4b e2 df 0c d0 5b c4 44 a8 e8	zAH.OPK. ...[.D..

12/ In the encrypted handshake record, what is being encrypted? How?

Answer: In the encrypted handshake record, handshake messages and MAC addresses are concatenated and encrypted. They are sent to the server.

SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message		
Content Type: Handshake (22)		
Version: SSL 3.0 (0x0300)		
Length: 56		
Handshake Protocol: Encrypted Handshake Message		

0090	04 6e 5a 00 98 2e 52 ee b5 bc d1 c4 f5 63 f0 e3	.nZ...R.c..
00a0	44 29 f1 c6 ba 64 58 79 46 9e 3e c4 fd d7 9b 7a	D)...dXy F->....z
00b0	02 04 09 32 f6 1d 7a a1 2d cf d2 1a 18 64 29 14	...2...z.d).
00c0	03 00 00 01 01 16 03 00 00 38 29 a9 dc 11 5a 748)...Zt
00d0	7a 41 48 15 4f 50 4b e2 df 0c d0 5b c4 44 a8 e8	zAH.OPK. ...[.D..
00e0	e4 e5 12 b9 11 f6 b3 9a de b7 22 0d 3a 17 9a 83".:...
00f0	77 1c de ab f2 41 e7 2e ad d5 1c 5b a2 0d ab e4	w....A. ...[....

13/ Does the server also send a change cipher record and an encrypted handshake record to the client? How are those records different from those sent by?

Answer: Yes, the server's encrypted handshake contains all the handshake messages sent from the server. Other contains messages sent from client.

112	21.876168	128.238.38.162	216.75.194.220	SSLv3	258 Client Key Exchange, Change Cipher Spec, Encrypted Handshake
113	21.945667	216.75.194.220	128.238.38.162	SSLv3	121 Change Cipher Spec, Encrypted Handshake Message
114	21.954189	128.238.38.162	216.75.194.220	SSLv3	806 Application Data
122	23.480352	216.75.194.220	128.238.38.162	SSLv3	272 Application Data

> Frame 113: 121 bytes on wire (968 bits), 121 bytes captured (968 bits)

> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)

> Internet Protocol Version 4, Src: 216.75.194.220, Dst: 128.238.38.162

> Transmission Control Protocol, Src Port: 443, Dst Port: 2271, Seq: 2785, Ack: 283, Len: 67

Transport Layer Security

SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec

Content Type: Change Cipher Spec (20)

Version: SSL 3.0 (0x0300)

Length: 1

Change Cipher Spec Message

SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message

Content Type: Handshake (22)

Version: SSL 3.0 (0x0300)

Length: 56

Handshake Protocol: Encrypted Handshake Message

14/ How is the application data being encrypted? Do the records containing application data include a MAC? Does Wireshark distinguish between the encrypted application data and the MAC?

Answer: The symmetric encryption algorithm is used to encrypt the application data. Yes, the records containing application data include a MAC.

Wireshark did not distinguish between the encrypted application data and the MAC.

114	21.954189	128.238.38.162	216.75.194.220	SSLv3	806 Application Data
122	23.480352	216.75.194.220	128.238.38.162	SSLv3	272 Application Data

> Frame 114: 806 bytes on wire (6448 bits), 806 bytes captured (6448 bits)

> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)

> Internet Protocol Version 4, Src: 128.238.38.162, Dst: 216.75.194.220

> Transmission Control Protocol, Src Port: 2271, Dst Port: 443, Seq: 283, Ack: 2852, Len: 752

Transport Layer Security

SSLv3 Record Layer: Application Data Protocol: http-over-tls

Content Type: Application Data (23)

Version: SSL 3.0 (0x0300)

Length: 747

Encrypted Application Data: 7e8cdc7fe71d6d59c45ecae7bad064ec705ea592d4b82b35...

15/ Comment on and explain anything else that you found interesting in the trace.

Answer: The version of SSL used changes from SSLv2 in the initial ClientHello message to SSLv3 in all following message exchanges.

11 | Page

Computer Networks