

Encryption Report

Table of Contents

- [Introduction](#)
- [Methodology](#)
- [TLS Handshake Analysis](#)
- [Packet Details](#)

Introduction

The objective of this report is to share the timestamp and details of the ClientHello, ServerHello, and the Key Exchange messages exchanged during the TLS handshake. It will explain the purpose and significance of each message in the TLS handshake process. The report will also identify the source and destination IP addresses and port numbers for each packet in the handshake. Finally, it will confirm that packets are encrypted after the handshake is completed.

Methodology

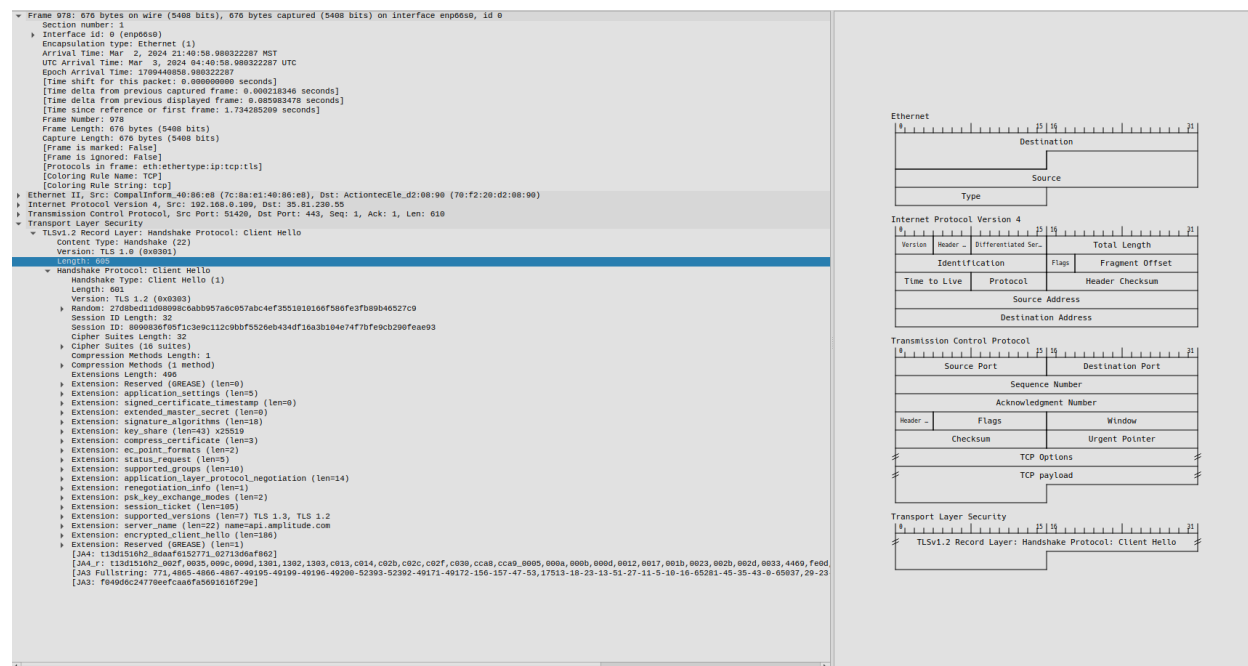
A. Tools Used

- Wireshark

B. Procedure followed

- Start Wireshark capture
- Filter on TLS handshake
- Identify ClientHello, ServerHello, and Key Exchange packets
- Examine packets to extract relevant information

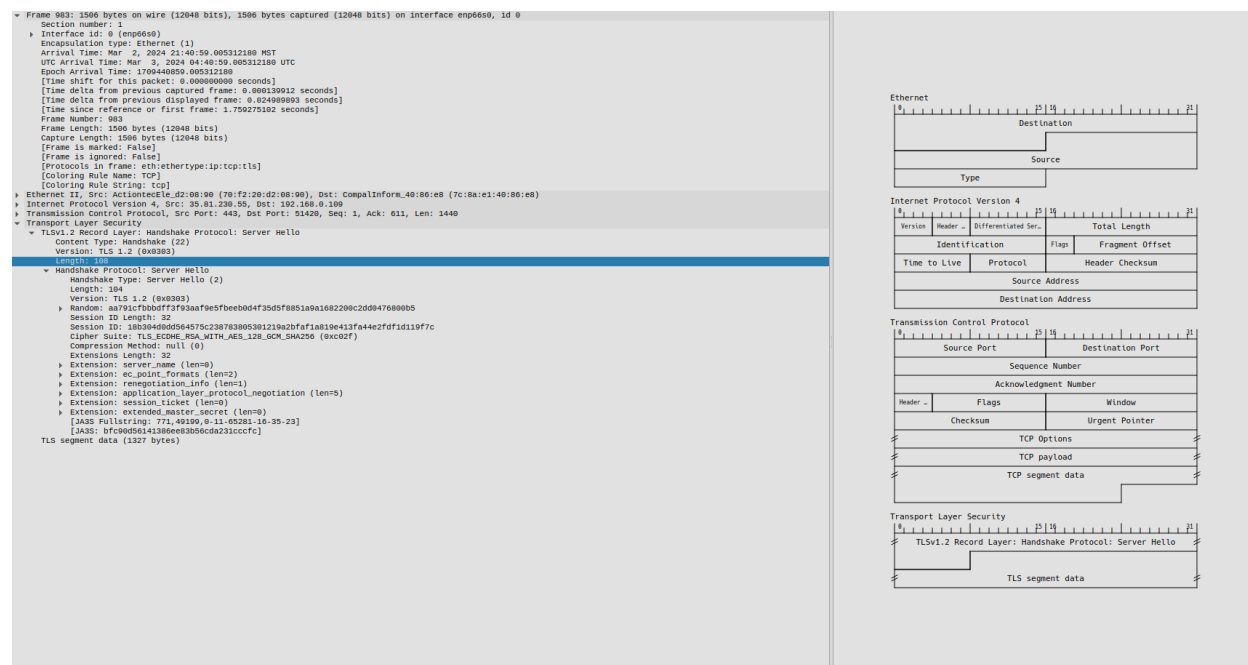
ClientHello Message



Purpose and Significance

- Initiates the TLS handshake by the client
- Proposes options for establishing the secure session:
- Contains a client random value used for key derivation and preventing replay attacks
- Allows server to select appropriate TLS options (version, ciphers, etc) supported by both parties
- Key exchange cannot begin until ServerHello is sent in response
- ClientHello must be the first message sent by client to negotiate TLS session

ServerHello Message



Purpose and Significance

- Confirms the version of TLS that will be used based on the options presented by the client.
- Chooses the cipher suite that will be used to encrypt data based on the client's options.
- Provides a random nonce value that will be used to derive symmetric keys.
- Indicates the server's chosen compression method from the client's options.
- Provides the server's certificate if certificate-based authentication is being used.

Key Exchange Message

▼ Frame 987: 868 bytes on wire (6944 bits), 868 bytes captured (6944 bits) on interface enp6s0, id 0

Section number: 1

Interface id: 0 (enp6s0)

Encapsulation Type: Ethernet (1)

Arrival Time: Mar 3, 2024 21:40:59.005671538 MST

UTC Arrival Time: Mar 3, 2024 04:40:59.005671538 UTC

Epoch Arrival Time: 1708440859.005671538

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.000261226 seconds]

[Time delta from previous displayed frame: 0.000359350 seconds]

[Time since reference or first frame: 1.709634400 seconds]

Frame Number: 987

Frame Length: 868 bytes (6944 bits)

Capture Length: 868 bytes (6944 bits)

[Frame is ignored: False]

[Protocols in Frame: eth:ethertype:ip:tcp:tls:x509sat:x509sat:x509sat:x509sat:x509sat:x509ce:x509ce:x509ce:x509ce:pkixexplicit:xm]

[Coloring Rule Name: TCP]

[Coloring Rule String: tcp]

Ethernet II, Src: ActiontecEle_d2:08:00 (7c:8a:e1:40:86:e8), Dst: CompalInform_40:86:e8 (7c:8a:e1:40:86:e8)

Internet Protocol Version 4, Src: 30.81.230.50, Dst: 192.168.0.100

Transmission Control Protocol, Src Port: 443, Dst Port: 51429, Seq: 4321, Ack: 611, Len: 802

[3 Reassembled TCP Segments (4662 bytes): #983(1327), #985(2880), #987(455)]

Transport Layer Security

▼ TLSv1.2 Record Layer: Handshake Protocol: Certificate

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 4657

Handshake Protocol: Certificate

Handshake Type: Certificate (11)

Length: 4653

Certificates Length: 4650

Certificates (4650 bytes)

Transport Layer Security

▼ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 333

Handshake Protocol: Server Key Exchange

Handshake Type: Server Key Exchange (12)

Length: 329

EC Diffie-Hellman Server Params

TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 4

Handshake Protocol: Server Hello Done

Handshake Type: Server Hello Done (14)

Length: 0

Ethernet

Destination

Source

Type

Internet Protocol Version 4

Version

Header

Differentiated Ser.

Total Length

Identification

Flags

Fragment Offset

Time to Live

Protocol

Header Checksum

Source Address

Destination Address

Transmission Control Protocol

Source Port

Destination Port

Sequence Number

Acknowledgment Number

Header

Flags

Window

Checksum

Urgent Pointer

TCP Options

TCP payload

Reassembled TCP Segments

Transport Layer Security

TLSv1.2 Record Layer: Handshake Protocol: Certificate

Transport Layer Security

TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange

TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done

▼ Frame 989: 192 bytes on wire (1536 bits), 192 bytes captured (1536 bits) on interface enp6s0, id 0

Section number: 1

Interface id: 0 (enp6s0)

Encapsulation Type: Ethernet (1)

Arrival Time: Mar 3, 2024 21:40:59.007132030 MST

UTC Arrival Time: Mar 3, 2024 04:40:59.007132030 UTC

Epoch Arrival Time: 1708440859.007132030

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.001454844 seconds]

[Time delta from previous displayed frame: 0.001450498 seconds]

[Time since reference or first frame: 1.761094958 seconds]

Frame Number: 989

Frame Length: 192 bytes (1536 bits)

Capture Length: 192 bytes (1536 bits)

[Frame is ignored: False]

[Protocols in Frame: eth:ethertype:ip:tcp:tls]

[Coloring Rule Name: TCP]

[Coloring Rule String: tcp]

Ethernet II, Src: CompalInform_40:86:e8 (7c:8a:e1:40:86:e8), Dst: ActiontecEle_d2:08:00 (7c:8a:e1:40:86:e8)

Internet Protocol Version 4, Src: 192.168.0.100, Dst: 30.81.230.50

Transmission Control Protocol, Src Port: 51429, Dst Port: 443, Seq: 611, Ack: 5123, Len: 126

Transport Layer Security

▼ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 78

Handshake Protocol: Client Key Exchange

Handshake Type: Client Key Exchange (10)

Length: 66

EC Diffie-Hellman Client Params

▼ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec

Content Type: Change Cipher Spec (20)

Version: TLS 1.2 (0x0303)

Length: 1

Change Cipher Spec Message

▼ TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 48

Handshake Protocol: Encrypted Handshake Message

Ethernet

Destination

Source

Type

Internet Protocol Version 4

Version

Header

Differentiated Ser.

Total Length

Identification

Flags

Fragment Offset

Time to Live

Protocol

Header Checksum

Source Address

Destination Address

Transmission Control Protocol

Source Port

Destination Port

Sequence Number

Acknowledgment Number

Header

Flags

Window

Checksum

Urgent Pointer

TCP Options

TCP payload

Transport Layer Security

TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange

TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec

TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

Purpose and Significance

- Allows client and server to securely share cryptographic key material
- Prevents encryption keys from being exposed on the network
- Enables derivation of symmetric keys used to encrypt session data
- Shared secret is used to derive symmetric encryption keys

- Prevents attackers from obtaining keys protecting session

Packet Details

A. Source and Destination Information

ClientHello Packet

- Source IP: 192.168.0.109
- Source Port: 51420
- Destination IP: 35.81.230.55
- Destination Port: 443

ServerHello Packet

- Source IP: 35.81.230.55
- Source Port: 443
- Destination IP: 192.168.0.109
- Destination Port: 51420

Key Exchange Packet

- Source IP: 35.81.230.55
- Source Port: 443
- Destination IP: 192.168.0.109
- Destination Port: 51420

B. Encryption Verification

The image displays a Wireshark packet capture analysis. The packet list shows a sequence of packets: 999 (ClientHello), 1000 (ServerHello), 1001 (KeyExchange), and 1002 (Application Data). The packet details pane for packet 999 shows the structure of the TCP segment, including the header, options, and payload. The packet bytes pane shows the raw data of the TCP segment.

Frame 999: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits) on interface enp6s0, id 0
Ethernet II, Src: RealtekU_82:00:00:70:12:30 (2:00:00:08:00:70:12:30), Dst: CompaqInfor_40:06:0b (7c:8a:14:40:06:0b)
Internet Protocol Version 4, Src: 192.168.0.109, Dst: 192.168.0.109
Transmission Control Protocol, Src Port: 443, Dst Port: 51420, Seq: 5372, Ack: 3533, Len: 248
Source Port: 443
Destination Port: 51420
[Stream index: 2]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 248]
Sequence Number: 5372 (relative sequence number)
Sequence Number (raw): 279578093
[Next Sequence Number: 5620 (relative sequence number)]
Acknowledgment Number: 3533 (relative ack number)
Acknowledgment Number (raw): 327605033
1080 = Header Length: 32 bytes (8)
Flags: 0x018 (PSH, ACK)
Window: 192
[Calculated window size: 40152]
[Window size scaling factor: 206]
Checksum: 0x7230 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
• TCP Option - No-Operation (NOP)
• TCP Option - No-Operation (NOP)
• TCP Option - Timestamp: Tsva1 3431237858, TSecr 3340980545
[Timestamps]
[SCS/ACK analysis]
[TCP payload: 248 bytes]
Transport Layer Security
• TLSv1.2 Record Layer: Application Data Protocol: HyperText Transfer Protocol 2

Frame 999, TCP payload (tcp.payload), 248 bytes.
Decod (R) = Show (A) = Start (0) = End (24)
Find: Find Next
Print Copy Save as Close Help