Detailed Packet Breakdown During Login

Aayush Adhikari
Roshan Tiwari
Shishir Rijal
Sudip Acharya

July 20, 2024

1 Detailed Packet Breakdown During Login

1.1 Ethernet Frame Header

Ethernet Frame

```
0000    c4 48 fa c5 de c0 90 65 84 05 43 03 86 dd 6b 80
```

Field	Value	Description
Destination MAC	c4:48:fa:c5:de:c0	Next hop device on local network
Source MAC	90:65:84:05:43:03	Sending device on local network
EtherType	86 dd	Payload is an IPv6 packet

1.2 IPv6 Header

IPv6 Header

```
0000                                                  6b 80
0010    00 00 07 18 06 40 24 00 1a 00 b1 e0 f6 ea 19 4f
0020    d9 1a b5 eb a1 4c 24 04 68 00 40 03 0c 01 00 00
0030    00 00
```

Field	Value	Description
Version	6	IPv6
Traffic Class	b8	QoS marking
Flow Label	000007	Identifies flows for QoS handling
Payload Length	18 (1816 bytes)	Length of IPv6 payload
Next Header	06 (TCP)	Type of next header
Hop Limit	40 (64)	Limits packet lifetime
Source IPv6	2400:1a00:b1e0:f6ea:194f:d91a	Sending host
Destination IPv6	b5eb:a14c:2404:6800:4003:c010	Receiving host

1.3 TCP Header

TCP Header

```
0030          00 00 00 5e d2 63 01 bb 7d 08 02 88 d3 0e
0040    e7 ac 50 18 02 00 42 57 00 00
```

Field	Value	Description
Source Port	`5e` (24162)	Sending process/application
Destination Port	`d2 63` (443, HTTPS)	Receiving process/application
Sequence Number	`01 bb 7d 08`	Orders data in byte stream
Acknowledgment Number	`02 88 d3 0e`	Next expected sequence number
Data Offset, Reserved, Flags	`e7`	TCP header length and control flags
Window Size	`ac` (172)	Available buffer space
Checksum	`50 18`	Error checking
Urgent Pointer	`02 00`	Last urgent data byte (not used)
Options	`42 57 00 00`	Additional TCP options

1.4 TLS Record Layer

TLS Record Layer

```
0040                                  16 03 01 06 ff 01
0050    00 06 fb 03 03 e1 ce b6 de 8b 30 de 2d cd 34 91
0060    7d a1 56 1c 07 69 e9 26 38 89 08 e9 e4 e4 8e d4
0070    c2 e6 22 88 50 20 66 91 cb 46 65 9b 17 d8 74 03
```

Field	Value	Description
Content Type	`16` (Handshake)	Type of TLS record
Version	`03 01` (TLS 1.0)	TLS version in record layer
Length	`06 ff` (1791 bytes)	Length of TLS record

1.4.1 TLS Handshake - Client Hello

Field	Value	Description
Handshake Type	`01` (Client Hello)	Initiates TLS handshake
Length	`00 06 fb` (1787 bytes)	Length of Client Hello message
Version	`03 03` (TLS 1.2)	Highest TLS version supported
Random	`e1 ce b6 de ... c2 e6 22 88`	Used for key generation
Session ID Length	`50` (80 bytes)	Length of Session ID field
Session ID	`20 66 91 cb ... 9b 0f d7 9c`	For session resumption

2 TLS Client Hello Analysis

TLS Client Hello Details

The TLS Client Hello message contains important information about the client's capabilities and preferences:

- **TLS Version:** TLS 1.2 (0x0303)
- **Client Random:** 32 bytes used for key generation
- **Session ID:** 80 bytes, suggesting session resumption capability
- **Cipher Suites:** List of encryption algorithms supported by the client
- **Compression Methods:** Indicates supported compression algorithms (usually null)
- **Extensions:** Additional features and capabilities supported by the client

Notable extensions observed:

- Server Name Indication (SNI): Specifies the hostname (accounts.google.com.np)
- Application Layer Protocol Negotiation (ALPN): Likely includes HTTP/2 support
- Supported Groups: Indicates supported elliptic curves for key exchange
- Signature Algorithms: Lists supported signature and hash algorithms
- Key Share: Pre-generates keys for faster handshake (TLS 1.3 preparation)

3 Security Analysis Overview

Security Aspects

- **IPv6 Usage:**
  - *Observation:* The packet uses IPv6, which is less common than IPv4.
  - *Implication:* May bypass some security controls not configured for IPv6.
- **HTTPS Connection:**
  - *Observation:* The destination port is 443 (HTTPS), indicating an encrypted connection.
  - *Implication:* Data transmission is likely secure from eavesdropping.
- **TLS Handshake:**
  - *Observation:* The packet contains a TLS Client Hello message.
  - *Implication:* The client is initiating a secure TLS connection.
- **Flow Label Usage:**
  - *Observation:* The IPv6 flow label is set.
  - *Implication:* May be used for QoS or load balancing, potentially affecting traffic prioritization.
- **Destination:**
  - *Observation:* The packet is destined for accounts.google.com.np
  - *Implication:* Attempting to log in to a Google account, from Nepal.
- **TCP Window Size:**
  - *Observation:* The TCP window size is relatively small (172).
  - *Implication:* Could indicate network congestion or a constrained device.
- **Packet Size:**
  - *Observation:* The payload length is 1816 bytes.
  - *Implication:* A large Client Hello message, possibly including many cipher suites or extensions.

4 Conclusion

This packet analysis reveals a standard TLS handshake initiation over IPv6 to a Google account service. While the use of TLS indicates a focus on security, the use of IPv6 and the specific destination highlight areas for potential security enhancements.