SYS-207 - Networks (Assessment Only)

00070 Assessment - Understand how transport protocols do protocol multiplexing, division into segments and reassembly of long messages, end-to-end performance control, assurance of (a) at-least-once delivery; (b) at-most-once delivery; (c) data

Name: Thanawin Pattanaphol ID: 01324096

Objective

Capture a traffic trace with Wireshark and identify where three End-To-End-Layer techniques appear in the trace, then, interpret one of those techniques in detail using the official protocol standards.

Captured Trace

The trace was captured on the eno1 interface, in this context, the Wi-Fi card; shown in Figure 1.

ply a display filter <					
Time	Source	Destination	Protocol		Info
213 8.207900	151.101.193.91	172.19.33.189	TLSv1.2		Application Data
214 8.207910	151.101.193.91	172.19.33.189	TLSv1.2		Application Data
215 8.207943	172.19.33.189	151.101.193.91	TCP TCP		50236 - 443 [ACK] Seq=3217 Ack=51585 Win=129664 Len=0 TSval=1847116695 TSecr=1757094732
216 8.207979 217 8.208929	172.19.33.189 151.101.193.91	151.101.193.91 172.19.33.189	TLSv1.2		50236 → 443 [ACK] Seq=3217 Ack=52678 Win=129792 Len=0 TSval=1847116695 TSecr=1757094732
217 8.208929	151.101.193.91	172.19.33.189	TLSV1.2		Application Data Application Data
219 8.208952	151.101.193.91	172.19.33.189	TLSV1.2		Application Data
220 8.209076	151.101.193.91	172.19.33.189	TLSv1.2		Application Data
221 8.209097	172.19.33.189	151.101.193.91	TCP		50236 → 443 [ACK] Seq=3217 Ack=55574 Win=128192 Len=0 TSval=1847116697 TSecr=1757094732
222 8.209120	172.19.33.189	151.101.193.91	TCP		50236 → 443 [ACK] Seq=3217 ACK=55374 Win=120192 Len=0 15Val=1847116697 TSecr=1757094732
223 8.209181	172.19.33.189	151.101.193.91	TCP		[TCP Window Update] 50236 → 443 [ACK] Seg=3217 Ack=57999 Win=131072 Len=0 TSval=184711669
224 8.217823	151.101.193.91	172.19.33.189	TLSv1.2		Application Data
225 8.217844	151.101.193.91	172.19.33.189	TLSv1.2		Application Data
226 8.217933	172.19.33.189	151.101.193.91	TCP		50236 → 443 [ACK] Seq=3217 Ack=60499 Win=128576 Len=0 TSval=1847116706 TSecr=1757094742
227 8.218045	151.101.193.91	172.19.33.189	TLSv1.2	1514	Application Data
228 8.218064	151.101.193.91	172.19.33.189	TLSv1.2	1119	Application Data
229 8.218220	172.19.33.189	151.101.193.91	TCP	66	50236 → 443 [ACK] Seq=3217 Ack=61947 Win=129664 Len=0 TSval=1847116706 TSecr=1757094743
230 8.218310	172.19.33.189	151.101.193.91	TCP	66	50236 → 443 [ACK] Seq=3217 Ack=63000 Win=130048 Len=0 TSval=1847116706 TSecr=1757094743
231 8.220883	151.101.193.91	172.19.33.189	TLSv1.2	1514	Application Data
232 8.220908	151.101.193.91	172.19.33.189	TLSv1.2	969	Application Data
233 8.220976	172.19.33.189	151.101.193.91	TCP	66	50236 → 443 [ACK] Seq=3217 Ack=65351 Win=128768 Len=0 TSval=1847116709 TSecr=1757094745
234 8.222803	151.101.193.91	172.19.33.189	TLSv1.2	1321	Application Data
235 8.222832	151.101.193.91	172.19.33.189	TLSv1.2		Application Data
236 8.222916	172.19.33.189	151.101.193.91	TCP		50236 → 443 [ACK] Seq=3217 Ack=66606 Win=129856 Len=0 TSval=1847116711 TSecr=1757094747
237 8.222999	151.101.193.91	172.19.33.189	TLSv1.2		Application Data
238 8.223077	172.19.33.189	151.101.193.91	TCP		50236 → 443 [ACK] Seq=3217 Ack=69113 Win=128576 Len=0 TSval=1847116711 TSecr=1757094747
239 8.224670	151, 101, 193, 91	172.19.33.189 04 bits), 138 bytes ca	TCP		443 → 50236 [ACK] Sen=69113 Ack=3217 Win=155648 Len=1448 TSval=1757094749 TSecr=184711676
ternet Protocol er Datagram Prot		::d3:00:33:c7:ea), Dst :1449:d389:1f7a:713e, Dst Port: 5353			0:88:00:fb)

Figure 1

End-To-End-Layer Techniques

To demonstrate the different End-To-End-Layer techniques shown in the Wireshark trace, this report will display three different techniques that can be found in this trace.

Connection establishment (TCP three-way handshake)

The Figure 2 shows a filtered Wireshark trace with the filter of tcp.flags.syn == 1 || tcp.flags.fin == 1, this filters packets such as [SYN], [SYN, ACK], and [ACK]

No.	Time	Source	Destination	Protocol	Length	Info				
	36 7.662670	104.21.20.105	172.19.33.189	TCP			FIN, ACK	[] Seg=80 Ack=92 Win=		
<u>_</u>	39 7.667739	172.19.33.189	151.101.65.91	TCP	78	50234 → 443	S [SYN, ECE	, CWR] Seq=0 Win=655		
	41 7.667958	172.19.33.189	104.21.20.105	TCP	66	50229 → 443	B [FIN, ACK	Seq=116 Ack=81 Win		
	43 7.671480	151.101.65.91	172.19.33.189	TCP	74	443 → 5023	4 [SYN, ACK	Seq=0 Ack=1 Win=65		
	45 7.677701	172.19.33.189	151.101.65.91	TCP	78	50235 → 44	3 [SYN, ECE	, CWR] Seq=0 Win=655		
> F	rame 43: Packet, 7	74 bytes on wire (59)	2 bits), 74 bytes capt	tured (592 bit	s) on inte	rface en0,	id 0			
> E	thernet II, Src: 6	52:a7:79:9a:7b:d4 (62	2:a7:79:9a:7b:d4), Dst	: Apple_d8:d0	:cb (98:01	:a7:d8:d0:cl	o)			
> I	nternet Protocol \	/ersion 4, Src: 151.:	101.65.91, Dst: 172.19	33.189						
~ T	ransmission Contro	ol Protocol, Src Port	t: 443, Dst Port: 5023	34, Seq: 0, Ac	k: 1, Len:	0				
_	Source Port: 443									
	Destination Port	: 50234								
	[Stream index: 1	.1								
	[Stream Packet N	lumber: 2]								
>	[Conversation co	mpleteness: Incomple	te, DATA (15)]							
	[TCP Segment Len	: 0]								
	Sequence Number:	<pre>0 (relative sequ</pre>	ence number)							
	Sequence Number	(raw): 2791431454								
	[Next Sequence N	lumber: 1 (relativ	e sequence number)]							
	Acknowledgment N	lumber: 1 (relativ	e ack number)							
Acknowledgment number (raw): 239799893										
	1010 = Head	er Length: 40 bytes	(10)							
>	Flags: 0x012 (SY	N, ACK)								
	Window: 65535									
	[Calculated wind	ow size: 65535]								
Checksum: 0xacac [unverified]										
[Checksum Status: Unverified]										
	Urgent Pointer: 0									
>	> Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale									
>	[Timestamps]									
>	[SEQ/ACK analysi									
	[Client Contiguo									
	[Server Contiguo	us Streams: 1]								
			*							

Figure 2

The three-way handshake synchronizes sequences numbers (ISS/IRS) and brings the endpoints to the ESTABLISHED TCP state; it prevents old duplicate segments from causing false connections [1].

Segmentation & Reassembly of long messages

Time	Source	Destination	Protocol	Length	Info	
3 7.689966	151.101.65.91	172.19.33.189	TCP	66	443 → 50234	[ACK] Seq=1550 Ack=3601 Win=1525
4 7.690431	172.19.33.189	151.101.193.91	TCP	1514	50236 → 443	[ACK] Seq=1 Ack=1 Win=131776 Ler
5 7.690433	172.19.33.189	151.101.193.91	TLSv1.2	970	Client Hello	(SNI=api.accounts.firefox.com)
	151 101 05 01	170 10 00 100	710.4.0	404		
		wire (12112 bits), 15:				
		(98:01:a7:d8:d0:cb),			(62:a7:79:9a:	:7b:d4)
		: 172.19.33.189, Dst:				
		rc Port: 50236, Dst Po	ort: 443, Seq:	1, Ack: 1,	, Len: 1448	
Source Por						
	n Port: 443					
[Stream in						
	cket Number: 4]					
		complete, DATA (15)]				
	nt Len: 1448]					
	umber: 1 (relativ					
	umber (raw): 3696114					
		(relative sequence n	umber)]			
	ment Number: 1 (r					
	ment number (raw): 2					
	= Header Length: 32	bytes (8)				
> Flags: 0x0						
Window: 20						
	d window size: 13177					
	ze scaling factor: 6	4]				
	0xa5e8 [unverified]					
	Status: Unverified]					
Urgent Poi						
		ion (NOP), No-Operati	on (NOP), Time	stamps		
> [Timestamp						
> [SEQ/ACK a						
	ntiguous Streams: 1]					
	ntiguous Streams: 1]					
	d (1448 bytes)					
	<u>ed PDU in frame: 75]</u> t data (1448 bytes)					

Figure 3

Figure 3 displays a reassembled packet, a demonstration of a large application payload across multiple TCP segments because of MSS/MTU limitations. The receiver uses sequences number and the TCP stream to reassemble the contiguous byte stream before delivering it to the higher-level protocol. This is an end-to-end functionality implemented by TCP and used by application protocols which is described in RFC 793 standard [2].

Retransmission (loss recovery to at-least-once delivery behavior)

Figure 4 shows a TCP Retransmission packet, this happens when TCP detects missing ACKs and retransmits the unacknowledged segment to ensure delivery. This provides the reliability property. RFC 973 discusses retransmission expectations and sequence number handling. [3]

```
196 8.193716
286 8.876308
                                         151.101.193.91
151.101.193.91
                                                                                 172.19.33.189
172.19.33.189
                                                                                                                                                      364 [TCP Retransmission] 443 → 50238 [PSH, 1514 [TCP Retransmission] 443 → 50238 [ACK]
              9.358861
9.524475
                                         172.19.33.189
104.21.20.105
                                                                                 104.21.20.105
172.19.33.189
                                                                                                                        TCP
TCP
                                                                                                                                                              [TCP Retransmission] 50239 → 443 [PSH, [TCP Retransmission] 443 → 50239 [PSH,
Frame 84: Packet, 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id 0 Ethernet II, Src: 62:a7:79:9a:7b:d4 (62:a7:79:9a:7b:d4), Dst: Apple_d8:d0:cb (98:01:a7:d8:d0:cb) Internet Protocol Version 4, Src: 151.101.193.91, Dst: 172.19.33.189
Transmission Control Protocol, Src Port: 443, Dst Port: 50236, Seq: 1, Ack: 2353, Len: 1448
     Source Port: 443
     Destination Port: 50236
     [Stream index: 3]
[Stream Packet Number: 8]
      [Conversation completeness: Incomplete, DATA (15)]
     [TCP Segment Len: 1448]
     Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2934957499
[Next Sequence Number: 1449 (relative sequence number)]
Acknowledgment Number: 2353 (relative ack number)
Acknowledgment number (raw): 3696117127
     1000 .... = Header Length: 32 bytes (8) Flags: 0x010 (ACK)
     Window: 292
[Calculated window size: 149504]
     [Window size scaling factor: 512]
Checksum: Øxebec [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
     Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
     [Timestamps]
    [SEQ/ACK analysis]
[Client Contiguous Streams: 1]
[Server Contiguous Streams: 1]
TCP payload (1448 bytes)
                                              ent data (1448 bytes)
```

Figure 4

References

- [1] J. Postel, *Transmission Control Protocol*, RFC 793, Internet Engineering Task Force (IETF), Sep. 1981. (See §3.4 "Establishing a Connection", pp. 27–31 for TCP three-way handshake and ISN synchronization.)
- [2] J. Postel, *User Datagram Protocol*, RFC 768, Internet Engineering Task Force (IETF), Aug. 1980. (UDP transport multiplexing description.)
- [3] J. Postel, *Internet Protocol*, RFC 791, IETF, Sep. 1981. (End-to-end fragmentation and reassembly rules pp. 13–23.)