COMP 416: Computer Networks

Project 2

Hasan Can Aslan – 60453

**Part 1A. SSL Implementation and Experiments**

**Question 1.** For each number, transmitted packets as follows:

**Graphical user interface, application, table

Description automatically generated**

18 TCP, 13 TLSv1.3 packets transmitted for each number. TLS requires TCP, so in total 31 TCP packets are transmitted for each number. Therefore, 155 TCP packets are transmitted in total while my KUSIS ID number is exchanged.

**Question 2.** My client supports 49 cipher suites. It can be found in the “Client Hello” message.

Text

Description automatically generated

**Question 3.** My client’s first message “Client Hello” indicates the last supported version, which is TLSv1.3. So, my client supports all TLS versions up to v1.3.

Graphical user interface, text

Description automatically generated

**Question 4.** Server will be using TLS\_AES\_256\_GCM\_SHA384 cipher suite. Hex dump of key is 0x1302.

Text

Description automatically generated

**Part 1B. SSL vs TCP: Delay Measurements**

**Question 5.** I get timestamp both sending the request and after receiving the server response. This graph shows the time difference of these timestamps for each message “1” and “2” in 5 trials.

|  |  |  |
| --- | --- | --- |
|  | "1" | "2" |
| 1 | 233ms | 358ms |
| 2 | 221ms | 326ms |
| 3 | 223ms | 309ms |
| 4 | 232ms | 330ms |
| 5 | 231ms | 310ms |

**Part 2. TCP Experiments**

**Question 6.** When a server starts a TCP connection, it assigns a random initial sequence number in range 0 and 232. Nonetheless, Wireshark displays relative sequence number instead of number assigned from host. Relative ACK Number is the number that Wireshark displays that relative to initial sequence number. In this way, we can keep track of sequence numbers easily.

**Question 7.** 149066.

A picture containing text, screenshot, black

Description automatically generated

**Question 8.** 44.

Text

Description automatically generated

**Question 9.** Same for all 6, 0.092 ms.

Chart, scatter chart

Description automatically generated

EstimatedRTT = (1 – α) • EstimatedRTT + α • SampleRTT

**Question 10.** Stream index in the TCP header identifies unique TCP stream. It is an internal mapping in Wireshark.

Graphical user interface, text

Description automatically generated

**Part 2. UDP Experiments**

**Question 11.** Source socket address is my IP address and port number which is 192.168.1.108:57342 and destination is OpenDNS server IP address and port number which is 208.67.222.222:53. We can find this information under DNS header.

Text

Description automatically generated

**Question 12.**

**A screenshot of a computer

Description automatically generated**

**Question 13.** I connected to local DNS server works in recursive manner because my client asks to local DNS server for IP address corresponding to nyu.edu. If it works in iterative manner, it should connect to “.” Which is root name server then, .edu server, contacts next name server up to the find requested IP address.

Recursive DNS is much faster, but it is vulnerable to attacks and unauthorized usage. In recursive, client only send query to 1st server.

**Question 14.** I get 1 response to my request. I get A Record for IP. It is public IP address and uses IPv4. It points to domain of IP address.

**Graphical user interface, text

Description automatically generated**

**Question 15.** Most common DNS types are: Mail exchanger record (MX Record), Canonical Name record (CNAME Record), Address Mapping record (A Record), Mail exchanger record (MX Record), Text Record (TXT Record), Name Server records (NS Record).

When using nslookup we can specify the type of DNS record using -type flag. For example, nslookup -type=NS www.nyu.edu.

Text

Description automatically generated Text

Description automatically generated

Text

Description automatically generated