Nova Southeastern University

College of Computing and Engineering

Assignment 2

ISEC 660 Advanced Network Security

Winter 2021

Due date: 2/14/2021

Total Points: 100

Notes:

1. Please include your name in EVERY document you submit.

2. Please sign and submit the “Certification of Authorship” form (located in Canvas) along

with your solutions.

Section I. Reading

1. PowerPoint Slides (accessed in Canvas)

2. (Suggested textbook)

ISBN: 978-0133594140

Computer Networking: A Top-Down Approach

Author: James F. Kurose & Keith W. Ross

Edition: 7th

Publisher: Prentice Hall

Year Published: 2016

(Chapters 1 – 5 of the textbook, okay to use the previous editions of the textbook)

Alternatively, you can refer to the following online materials by focusing on the Application Layer,

the Transport Layer, the Network Layer (layer 3), and the Datalink layer (layer 2) of the protocol

stack.

https://www.geeksforgeeks.org/computer-network-tutorials/

https://www.javatpoint.com/computer-network-tutorial

Section II. Questions (80 points, all questions are equally weighted)

Q1. What is a network protocol?

A Protocol is used to determine a set of rules to communicate over a network. If devices are connected protocols allow them to exchange data regardless of architecture and design.

Q2. Why does the HTTP protocol run on top of TCP rather than on UDP?

HTTP runs on the Transmission Control Protocol because HTTP uses connection-oriented architecture. If you send a request to HTTP via TCP it will give you a definitive answer on its return, some typical types of HTTP responses are 200 OK, 403 Forbidden, or 404 Not Found. The beauty of this is you get a response to your request which can help you determine how to proceed. Whether it succeeded or failed, you get a clue in the response of what happened. The disadvantage of UDP rather than TCP is you are not guaranteed a response. So, if you sent a request to HTTP via UDP and it did not work or return anything you would have no idea why. There is no guarantee that UDP will deliver a response to why it was failing or even if it succeeded. This is not good when accessing HTTP because you want a guaranteed connection for transactions and also information on why connection failed or if it succeeded, UDP does not provide this.

Q3. What are the two major services provided at the transport layer? What are their differences?

The two major services at the transport layer are User Datagram Protocol (UDP) and Transaction Control Protocol (TCP). The simplest explanation of their major’s differences is that TCP is a connection-oriented protocol, while UDP is connectionless. A real-world comparison of this would be that TCP is like a phone call, there is a guaranteed connection between two parties before exchanging information. TCP guarantees a connection before proceeding forward. Where UDP is more like a radio broadcast, it sends out data with out any guarantee the receiver heard it. So UDP will transmit data with no guarantee that the receiver is even listening or ready to return data.

Q4. Suppose Client A initiates a SSL session with server S. Provide possible source and destination

port numbers for:

1. The segment sent from S to A.

Server Source Port# 443, Client Destination Port #1467

1. The segment sent from A to S.

Client Source Port# 1467, Server Destination Port #443

Q5. Describe two major network-layer (layer 3) functions in a datagram network.

The two major network-layer functions in a datagram network are forwarding and routing. Routing will determine the routes between the source and destination devices on a network. These are typically stored in a routing table and give a detailed view of how the protocol will hop from devices when transmitting a packet on a network. This is routed through the whole network and not just locally on one device. In contrast, a forward is a router local action where packets are forwarded from the routers source input link to the appropriate destination output link.

Q6. Briefly compare and contrast IPv4 and IPv6.

Both IPv4 and IPv6 are forms of IP addresses to determine a device on the network. IPv4 is based of off 32-bit integers in 4 sets of 8 bits called octets. IPv6 is based off of 128-bit integers and uses hexadecimal code to store 4 numbers in a group of 8 containing 32 numbers. IPv6 was created because IPv4 will soon be full and no more address will be able to be created so engineers invented IPv6 because it can hold up to 1028 times more addresses then IPv4. So, although they both store IP addresses IPv6 can hold significantly more addresses than its predecessor.

Q7. Suppose an application generates chunks of 1960 bytes of data every 20 millisecond, and

each chunk gets encapsulated in a TCP segment and then an IPv4 datagram. Assuming that all

TCP segments and IPv4 datagrams use default structures for headers. What percentage of each

datagram will be overhead, and what percentage will be application data?

Application generates 1960 bytes.

TCP segment address adds 20 bytes and IP adds 20 bytes.

Overhead bytes = (20 TCP bytes +20 Ip Address bytes) = 40 Bytes.

So total bytes = (20 TCP bytes +20 Ip Address bytes + 1960 Application Bytes) = 2000 Bytes total.

Percentage of datagram used for headers = (40 bytes / 2000 bytes) = .02

So, 2% will be overhead and 98% will be application data.

Q8. Why the Ethernet is called a multiple access protocol? Is it a reliable protocol or not? Why?

Ethernet is called the multiple access protocol because it uses Carrier Sense, Multiple Access with Collision Detect (CSMA/CD) and even has “multiple access “in the name. Ethernet is a multiaccess network where multiple nodes can send and receive frames over a shared link. This is essentially a bus with multiple nodes plugged into. Ethernet is a reliable protocol because it typically has larger transfer sizes and speeds compared to Wi-Fi. It is also more reliable because it is less susceptible to packet drops over its hard wire compared to packets dropping more consistently over Wi-Fi. Lastly, Ethernet is considered relatively secure compared to Wi-Fi because an attacker would physically have to plug into the network rather than hacking it digitally.

Q9. What is the major networking device at the network layer (layer 3)? What is the major

networking device at the datalink layer (layer 2)?

The major networking device on the datalink layer (layer 2) is a switch. This device routes traffic based off the connecting devices Media Access Control Address (MAC address). This is its layer 2 address and does not need a layer 3 IP address for its routing only its physical MAC address. The major networking device for the network layer (layer 3) is a router. This device routes traffic based off of the devices network IP addresses rather then their physical MAC address. The difference being that layer 2 switches are based of MAC addresses while Layer 3 routers are based of network IP addresses.

Q10. Why are acknowledgements (i.e. receivers acknowledging the recipient of messages) used

in 802.11 but not in a wired Ethernet?

Section III. Practical assignment (20 points)

In this Wireshark lab, you’ll get acquainted with Wireshark, and make some simple packet

captures and observations. A brief introduction of the Wireshark tool, its installation, and initial

experiments can be found in the file “Wireshark\_Intro.pdf”.

You are required to install the latest version of Wireshark, run the tool, and capture network

traffic by accessing http://www.mit.edu/index.html. It is recommended that you disable other

background networking applications to make the traffic easy to identify. Answer the following

questions:

1. What is the IP address (IPv4 or IPv6, depending on the platform you used) and TCP port

number used by the client computer (source) to communicate with www.mit.edu? What

is the IP address (IPv4 or IPv6) and TCP port number used by the server (destination)

www.mit.edu?

2. What is the sequence number of the TCP SYN segment that is used to initiate the TCP

connection between the client computer and nsu.nova.edu? What is it in the segment that

identifies the segment as a SYN segment?

3. How long did it take from when the HTTP GET message was sent until the HTTP OK

reply was received? (By default, the value of the Time column in the packet-listing

window is the amount of time, in seconds, since Wireshark tracing began. To display the

Time field in time-of-day format, select the Wireshark View pull down menu, then select

Time Display Format, then select Time-of-day.)

4. Print the two HTTP messages (GET and OK) referred to in question 3 above. To do so,

select Print from the Wireshark File command menu, and select the “Selected Packet

Only” and “Print as displayed” radial buttons, and then click OK.

5. Print the two TCP messages (SYN and SYNACK) referred to in question 2 above.

6. Is the connection to nsu.nova.edu secure or not? Why? Justify your answer based on the

captured network traffic.



Certification of Authorship of Assignment

Submitted to (Professor’s Name): Dr. Wei Li

Class/Semester: ISEC660 Advanced Network Security, Winter 2021.

Students’ Names: Eric Webb

Date of Assignment: 2-14-2020

Title of Assignment: Assignment #2

Certification of Authorship: By submitting this document we certify that we are the authors of this paper and that any assistance we received in its preparation is fully acknowledged and disclosed in the paper. We have also cited any sources from which we used data, ideas or words, either quoted directly or paraphrased. We also certify that this paper was prepared by us specifically for this course.

Students’ Signatures: Eric Webb