CS 494/594 Final Exam (Winter 2022) Portland State University
Instructor: Dr. Nirupama Bulusu

Name: Parth Parashar_____

There are five questions in this exam. Your answers can either be typed or handwritten. Once you complete the exam, please upload the completed exam on Canvas. All paper PDFs referenced are in the final exams folder on Canvas.

SUBMISSION DEADLINE: Friday, Mar 17th, 2022 11:59 pm PST.

Please plan ahead and try to submit your final exam a few days or few hours early.

1. **(20 points)** Protocol Perils
Read the following paper.
[Georgiev12.pdf]
Martin Georgiev, Subodh Iyengar, Suman Jana, Rishita Anubhai, Dan Boneh, and Vitaly Shmatikov. 2012. The most dangerous code in the world: validating SSL certificates in non-browser software. In Proceedings of the 2012 ACM conference on Computer and communications security (CCS '12).

(i) What is the type of attack that results from broken SSL certificate validation? Explain how this attack works.

Answer: - The attack that results from a broken SSL certificate validation is the **Man in the Middle Attack.**

A man in the middle attack can be defined as an attack when a particular hacker/attacker comes in between two parties and starts decoding messages between those two parties to steal/gain important information. The attacker/hacker also starts sending messages to the other party, but they think that it has indeed come from the correct machine.

For example: - There is an exchange of sensitive information (let's suppose credit card details) between A and B. Also, let us suppose that B's system has a broken SSL certificate validation.

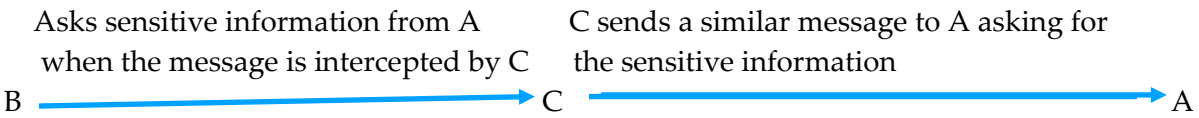
When A sends a message to B asking for sensitive information (credit card details), the attacker (Named C) intercepts the traffic, decodes the message, and now knows that A is expecting sensitive information (credit card details) from B.
Consequently, C sends fake message to B which looks similar to the original message, making it seem like it was sent by A.

Now, since B's system has a broken SSL certification validation, it cannot check whether the message originated from A's machine or not.

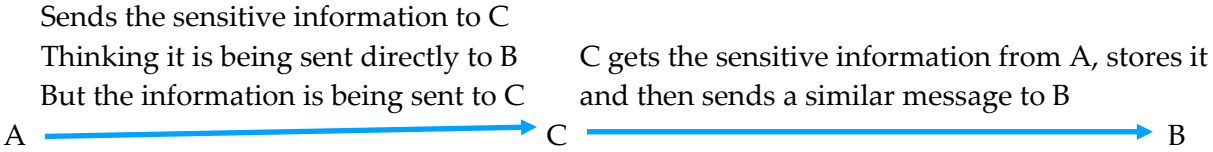
This means that B believes that the message was sent by A and sends the sensitive information (credit card details) across the network thinking it is going directly to A. But the information is going to A through C who will steal the information and use it to his/her benefit.

Both A and B think that they have sent and received information safely but in actuality, the information was intercepted by C .

This can be written as: -
Step-1: -



Step-2: -



(ii) What attacker capabilities and threat model do the authors assume?

Answer: - Attacker Capabilities: -

1) They are a man in the middle, network attacker who may control network routers or switches, WiFi access points or DNS.
2) They may also control one or more servers and they might also possess valid SSL certificates for these servers.
3) The attacker may also mislead server's network address through DNS poisoning.

The author assumes the following threat model: -

1) The attackers do not possess any access to the private keys of the legitimate servers.
2) The attackers do not control any certificate authority
3) The attackers cannot forge any certificates
4) A correctly implemented SSL client would refuse to accept any malicious server certificates because of the mismatch between the name on the server and the certificate name.

(iii) Of the recommendations the authors propose to address these threats, which do you think is the most feasible? Why?

Answer: - The recommendation for application developers would be to use fuzzing and adversarial testing to check how the application behaves with abnormal SSL certificates.
This can be attributed to the following reasons: -

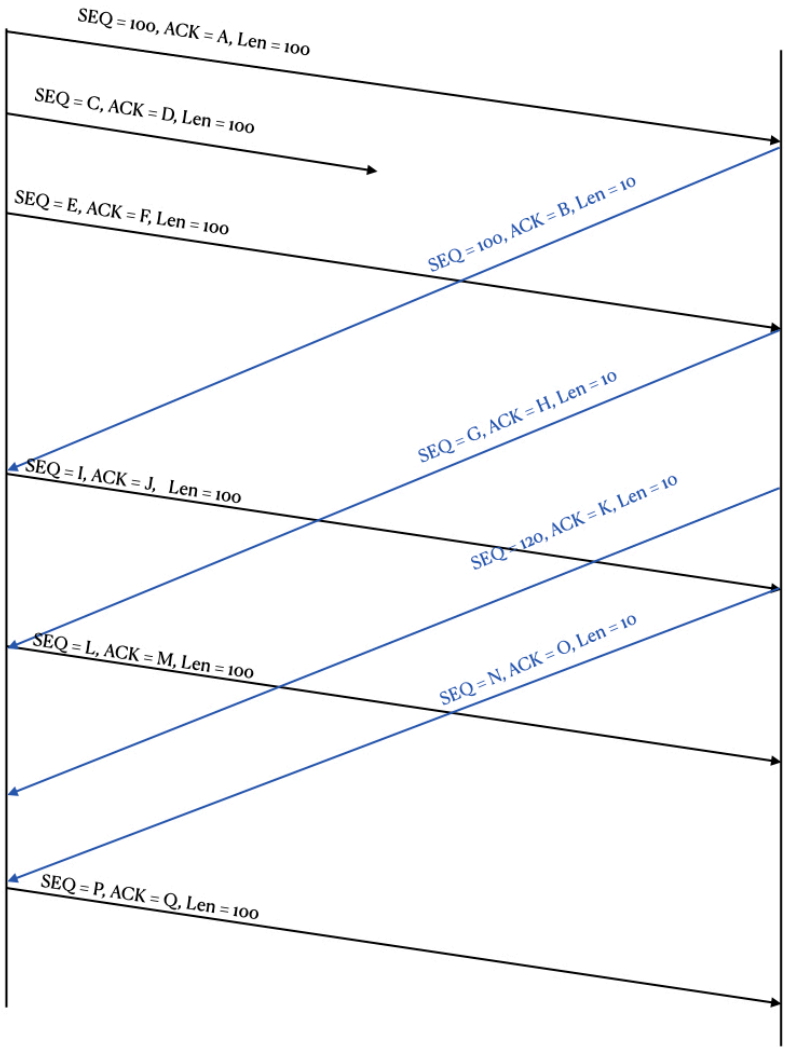
1) If we have enough fuzzing and adversarial tests, we would be making sure that we cover a lot of the edge cases and scenarios where there might be a use of abnormal SSL certificates. And if the testing fails, we are sure that there is some issue.
2) If there are enough tests, we can also detect what happens when we make requests with untrusted certificates, the response from the service should fail, and it that doesn't happen, we know that we haven't reverted disabling the certificate validation which was done during testing.
3) Similarly, if we have tests written to test for multiple versions of the SSL library, we can test the same thing, if it passes with wrong parameters, we know that there is something wrong with the new versions. All these tests can be automated, which takes the burden of manual errors. It is a one-time setup, which will benefit the company/team hugely in the long run

The most feasible recommendation for SSL library developers is to make SSL libraries more explicit about the semantics of their APIs.
And this is most feasible because of the following:

1) authors state that application developers do not understand the meaning of various options, and use it wrongly, because of which they end up sometimes either disabling certificate verification or end up not doing proper checks.
2) By not delegating the responsibility of SSL connections to applications, the SSL libraries are assuming a lot of the variables, which can lead to developers moving away from the library itself. This is because, different applications have different needs, and you cannot assume for them
3) There are various SSL libraries out there, some are built as a side project, some for the sole purpose of certain companies. And these errors and interfaces very much depend on the different languages, different hierarchies they have. There can never be one way to do this.

2. **(20 points)** Complete the missing sequence numbers (Seq), acknowledgement numbers (ACK), and segment length (LEN) in the following TCP Reno sender, receiver connection.

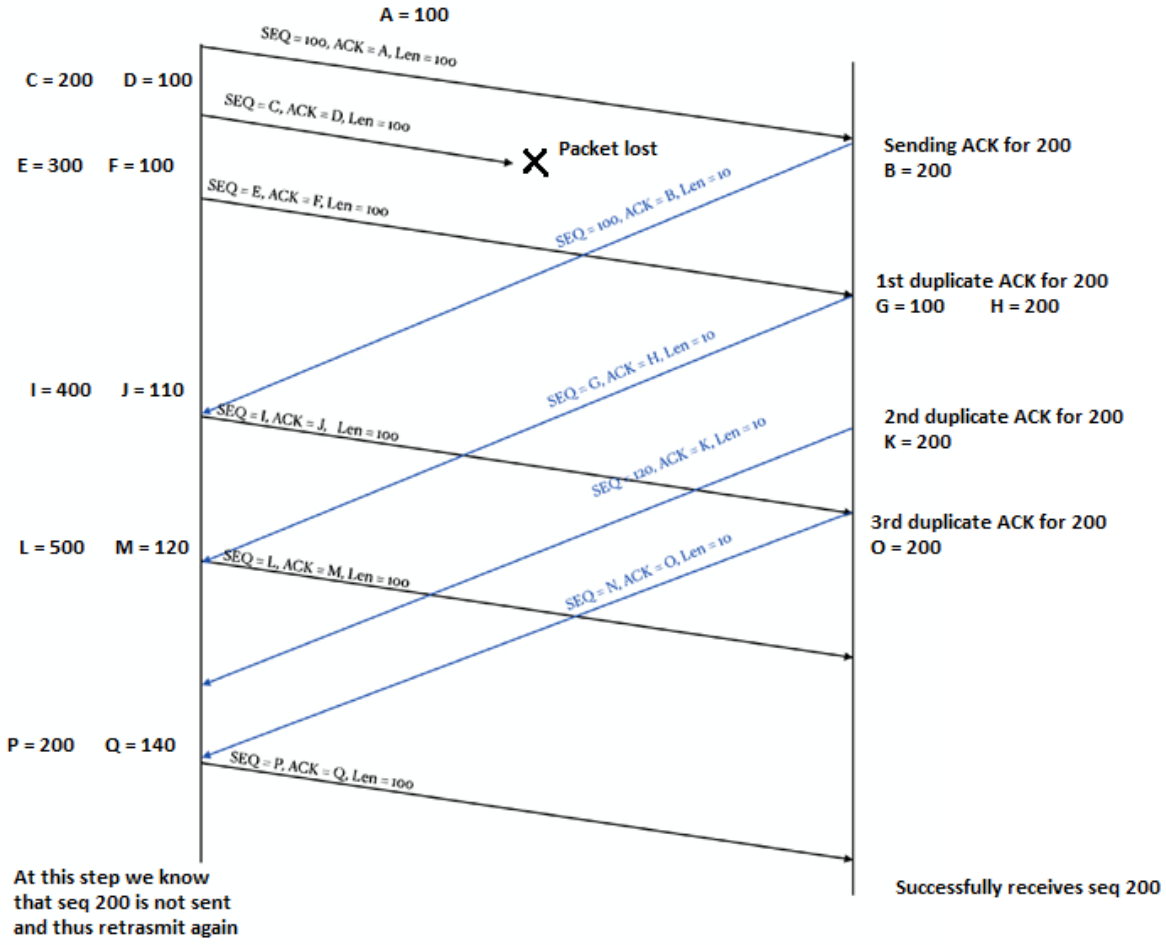
Assume: (i) No timeouts occur. (ii) The connection is full-duplex. (iii) The sender and receiver always have data to transmit. (iv) There are no delayed acknowledgements at the



sender or receiver. (v) The initial TCP handshake has already been completed.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q

Answer:-



This is a full duplex connection where the sender and receiver transmit data all the time. Here there is no timeouts, and the sender realizes that a packet is lost if 3 duplicate acknowledgements are sent to the sender from the receiver after the initial handshake has been completed.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
100	200	200	100	300	100	110	200	400	110	200	500	120	130	200	200	140

3. (20 points) BGP

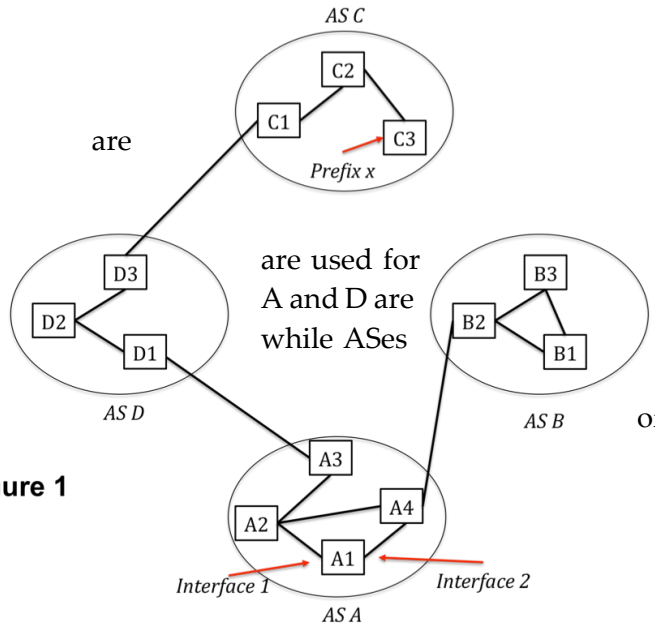


Figure 1

Consider the network in Figure 1, with ASes A, B, C, D. Each AS has some number of routers (labeled as$A1,$A2, etc.) and the domains connected internally and with each other by the links depicted in the figure. Assume that eBGP and iBGP are used for inter domain routing, and that ASes A and D are using RIP for intradomain routing while ASes B and C are using OSPF for intradomain routing. Prefix x hangs off an interface on router C3.

i) Router D3 learns about prefix x from which routing protocol: OSPF, RIP, eBGP, or iBGP?

Answer: - Router D1 learns about prefix x from iBGP (Internal Border Gateway Protocol)

ii) Router D1 learns about prefix x from which routing protocol?

Answer: - Router D3 learns about prefix x from routing protocol eBGP (External Border Gateway Protocol)

iii) Router A3 learns about prefix x from which routing protocol?

Answer: - The router A3 learns about prefix x from eBGP (External Border Gateway Protocol). Since we know that routers use eBGP to communicate to routers between two autonomous system. As the A3 is directly connected to autonomous system D through which A3 learns about the prefix X in the autonomous systems C

iv) Router A1 learns how to reach router A3 from which routing protocol?

Answer: - Router A1 learns how to reach router A3 from RIP (Routing Information Protocol).

v) Will router A1 use interface1 or interface2 to reach prefix x?

Answer: - The router A1 will use interface 1, as the autonomous system A is connected to autonomous system D through interface 1, which is in turn connected to autonomous system C where the prefix X is connected to the router C3

4. **(20 points)** Virtual LANs

Network segmentation using virtual LANs has been proposed as a method to protect vulnerable corporations from sophisticated hackers. Research and identify one major network breach that could have been prevented by using virtual LANs. Ideally, how should the VLAN have been segmented to thwart the breach?

Answer: - One major breach that could have been prevented by using virtual LANs is a **malware used to perform ransomware attacks.**

GENERAL MALWARE ATTACK AND MALWARE: -

A malware attack is defined as a common cyberattack where a malicious software is installed on the victim's system with the help of a network, which then executes / runs unauthorized actions on the victim's system or organizations (which can include exploring, stealing or virtually conducting any operations on the victim's system).

RANSOMWARE: -

Ransomware is malicious software designed to block access to a computer system.
It infects your system, then locks or encrypts your most important data, allowing attackers to ask for a ransom.
The attackers will offer to provide the decryption key only if you pay a certain amount of money within a short time.

WORKING OF RANSOMWARE: -

Most ransomwares are usually delivered via an email which appears normal and legitimate.
The email generally consists of a link or attachment that then installs the malicious software onto the victim's computer.
Ransomware is also delivered via drive-by-download attacks on compromised or malicious websites.

Generic ransomware is rarely individually targeted, but rather a shotgun approach where attackers acquire lists of emails or compromised websites and blast out ransomware.

Given the number of attackers out there, it is quite possible that you will be hit multiple times and each time, it could be a different attacker altogether who performs the attack.

But Ransomware breaches are one of the most common breaches which can be prevented easily by using Virtual LANs

PREVENTION OF RANSOMWARE: -

There are a few actions that organizations can take to help mitigate risk and limit the fallout of a ransomware attack.

One of the most important solutions that can be used to prevent ransomware attacks is the use of network segmentation.

Network segmentation involves splitting the larger network into smaller network segments.

This can be done using firewalls, virtual local area networks (VLAN).

Segmentation lays the groundwork for controls that protect against lateral movement on the network by ransomware or hackers, preventing an infection or compromise from spreading across the network.

The major advantage of segmentation is that, even if a user ends up as a victim of phishing attack, it will only impact that segment and thus preventing a major network breach.

VLAN SEGMENTATION TO THWART THE BREACH: -

A VLAN is helpful for organizational use mainly because it can be used to segment a larger network into smaller segments.

VLANs can limit the user access to a certain VLAN, which then allows only authorized users to have access to networks with highly sensitive information.

As we know how segmentation helps in reducing the impact of Ransomware to only one segment even if the network is under Ransomware attack.

5. **(20 points)** IPv6 over IPv4

6to4 is an Internet transition mechanism for migrating from IPv4 to IPv6, a system that enables IPv6 packets to be transmitted over an IPv4 network (generally the IPv4 Internet) without the need to configure explicit tunnels. 6to4 is described in RFC 3056, *Connection of IPv6 Domains via IPv4 Clouds.* Describe the stages involved in IPv4 to IPv6 transition, using 6to4. What is the condition for removing the 6to4 configuration?

Answer: - IPV4 was being used extensively for a long period of time. Now, because of the increase in the number of internet users and subsequent increase in the number of websites as well, IPV4 was facing a major hurdle in the form of address exhaustion.

This is because IPV4 addresses are 32-bits long and is generally of the form xxx.xxx.xxx.xxx

Any set can take values ranging from 0 to 255. This means, the total number of addresses is equal to 256 raised to power 4. This is equal to 4.3 billion unique addresses.
While these may sound a lot, but in today's day and age when there are literally a large number of devices and each device needs a unique address to send and receive information over the internet, this is a very small number.

Hence, IPV6 was created. IPV6 addresses are 128 bits long which **significantly increases the number of devices which can be accommodated.**

6to4 is an internet-based mechanism for transitioning from IPv4 to IPv6.
The following stages are involved in the transition from IPv4 to IPv6

Address block allocation:

1) When a host receives a global IPv4 address, the IPv4 address is appended to the address block 2002::/16, resulting in a 48 bit 6to4 IPv6 prefix
2) An IPv6 address with the prefix 2002::/16 is called a 6to4 address.

Encapsulation and Transmission:

1) 6to4 encapsulates IPv6 packets for transmission across an IPv4 network. When protocol type 41 6to4 is used, IPv6 packets are inserted in the payload of an IPv4 packet.
2) When transferring an IPv6 packet over an IPv4 network, an IPv4 header with protocol type 41 is prepended to it. Extraction of 32 bits after the IPv6 destination address prefix yields the IPv4 destination address for the prepended packet header.
3) The host or router's IPv4 address appears as the IPv4 source address in the prepended packet header. Finally, the IPv4 packet reaches its proper destination

Routing traffic between 6to4 and native IPv6:

1) The relay router connects IPv4 and IPv6 networks, bridging the gap
2) IPv6 payloads will be routed to the IPv6 network for 6to4 packets arriving on IPv4, while packets coming from IPv6 interfaces with the prefix 2002::/16 will be encapsulated and forwarded on the IPv4 network.
3) Transitioning from 6to4 to IPv6 addresses is handled by relay routers. To get packets from the internet to the 6to4 system, IPv6 routing methods are used.