

ITIS 6200/8200 Principles of Information Security and Privacy

Homework 4

Please **briefly** explain your answer.

Question 1. ARP Attack (15 points)

ARP, the Address Resolution Protocol, translates Layer 3 IP addresses into Layer 2 MAC addresses. Assume that Alice wants to communicate with Bob, whose computer is on the same LAN network. Alice knows Bob's IP address but wants to learn his MAC address.

An attacker, Mallory, wants to convince Alice that her MAC address (and not Bob's) corresponds to Bob's IP address, causing messages intended for Bob to be sent to Mallory instead. Mallory, Alice, and Bob all use the same LAN network. Assume that (1) Mallory's computer has IP address 1.2.3.6 and Mallory's MAC address is 66:66:66:66:66:66, (2) Alice's IP address is 1.2.3.77 and her MAC address is 77:77:77:77:77:77, and (3) Bob's IP address is 1.2.3.8 and his MAC address is 88:88:88:88:88:88. The network LAN router's IP address is 1.2.3.4.

Q 1.1: Alice broadcasts to everyone else on the LAN: "What is the MAC address of 1.2.3.8 (Bob)?" What values for the IP and MAC address can Mallory include in her response to Alice to cause her messages intended for Bob to be sent to you instead?

Ans: Bob's IP address 1.2.3.8 and Mallory's MAC address: 66:66:66:66:66:66

Q 1.2: How would Mallory's spoofed response to Alice change if Bob was outside the LAN?

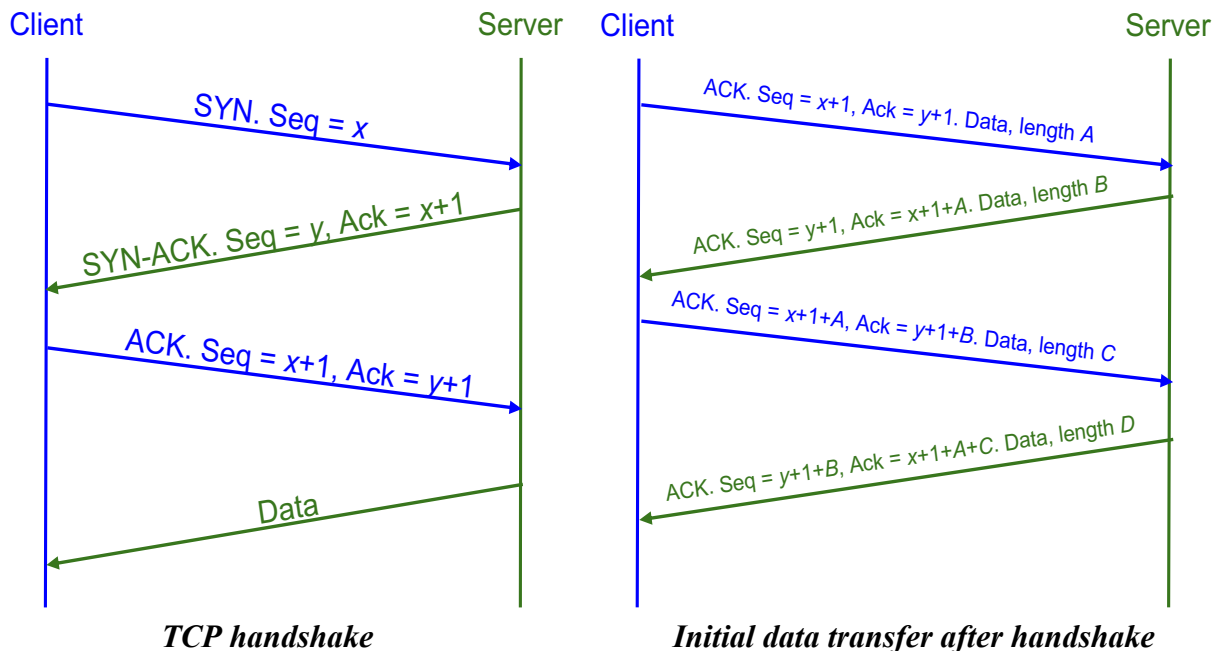
Ans: Use the IP address of the router: 1.2.3.4

Q 1.3: A network switch is deployed to prevent ARP spoof attacks. Describe what would the switch do in the following two cases: (1) the switch knows Bob's IP to MAC address mapping and (2) the switch does not know Bob's IP to MAC address mapping. Explain in one sentence why that helps with ARP spoof attacks.

Ans: The switch looks up in its table to find Bob's MAC address, if not there, it broadcasts all other computers. It helps with ARP by reducing the need of sending requests to other computers.

Question 2. TCP Spoofing (25 points)

The left diagram below shows how TCP handshake works. The right diagram show initial data have been transferred between the Client and the Server.



Q 2.1: Assume that the next transmission will be some data sent from Client to Server. What are the sequence number and ACK for this packet?

Ans: Seq #: $x+1+A+C$ ACK #: $y+1+B+D$

Q 2.2: Consider a on-path attacker Eve who can observe the traffic but cannot modify it. Can Eve hijack the TCP connection between the Client and the Server? What can she do?

Ans: Yes. Eve can spoof packets in both directions, using the server's IP and the client's IP. The recipient cannot distinguish it from the legitimate messages.

Q 2.3: Consider a off-path attacker David who cannot observe and modify the traffic. Can David do anything malicious to the connection? If so, what can he do?

Ans: No much David can do other than blend spoofing.

Q 2.4: The Client wants to send a message M to the Server. Consider a modified version of TCP where the Server no longer sends an ACK to the Client for messages the Server receives. If the Client sends a message M using this modified version of TCP and M was dropped during delivery, can the Server know that M is lost? Would the message M be resent by the client?

Ans: The server knows that M is lost, but the message won't be resent.

Q 2.5: The Client wants to send a message M to the Server. Consider a modified version of TCP where the Client no longer sends an ACK to the Server for messages the Client receives. If the client sends a message M using this modified version of TCP and M was dropped during delivery, can the Server know that M is lost? Would the message M be resent by the Client?

Ans: The server knows that M is lost, and the message will be resent since the client also knows from the Server's ACK.

Question 3. Denial of Service Attack and Firewalls (20 points)

SYN flooding attack is a DoS attack that attacks a server by sending a large amount of SYN requests to the server.

Q 3.1: Explain in two sentences how this DoS attack works. (What resources are being consumed at the server?)

Ans: The server allocates too much resources, i.e., memory, to keep track of all the states needed for each connection.

Q 3.2: The server wants to defend against SYN flooding attack by SYN cookies: it encodes the state needed for each SYN request as the sequence number of the SYN-ACK message sent back from the server. Assume the server needs to track the following information (or state) for each SYN request: (a) Source IP, (b) Source Port, (c) Destination IP, and (d) Destination Port. Design a scheme to generate a sequence number to encode and track the information. Explain how to validate the connection with such a sequence number.

Ans: There can be many answers. For example, do a hash function on (a)+#+(b)+#+(c)+#+(d) to produce a unique sequence number. To validate, when the client sends further ACK packet, do a hash and check if the sequence number match.

Q 3.3: Assume we want to use stateful packet filter to help with SYN flooding. Write a rule that allows inbound connections to IP address 1.2.3.4 with port 8080.

Ans: Allow TCP *.*/*ext -> 1.2.3.4:8080

Q 3.4: Reconsider Q 3.2 about encoding the information needed for a SYN request with a sequence number. How to use the generated sequence number to help with filtering suspicious packets?

Ans: Establishing connections and states only after the TCP handshake receives an ACK packet from the client with the right sequence number. Or attach the sequence number to some numbers, e.g., 99999, and filter out packets that don't have the prefix.

Question 4. Intrusion Detection (20 points)

Q 4.1: Explain the difference between specification-based detection and anomaly-based detection. Which has better false positive rate? Explain why in one sentence.

Ans: specification-based detection has better false positive rate. Anomaly-based detection may be incorrectly trained / built.

Q 4.2: Name an example system where the false positive rate may be more important than the false negative rate. Explain why in one sentence.

Ans: Online banking system.

Q 4.3: Name your favorite detection style, and explain why with an example system.

Ans: The answer may vary.

Q 4.4: Explain how to deal with the path traversal attack with the four different detection style. Make a bullet and explain how for each of the four different detection styles.

Ans: specification-based: specify what characters are allow: alphanumeric

Signature-based: doesn't allow ../

Anomaly-based: analyze characters in requests and learn that ../ only appears in attacks

Behavior-based: See if any unexpected files are being accessed (e.g. the passwords file)

Question 5. Memory Vulnerability (20 points)

Consider the following vulnerable C code. Assume you are on a little-endian 32-bit x86 system and no memory safety defenses are enabled.

```
1  #include <stdio.h>
2  #include <stdlib.h>
3
4  void foo(int a, int b){
5      ... int age;
6      ... char name [12];
7      ... printf("What is your name?\n");
8      ... gets (name);
9      ... printf("%s\n", name);
10 }
11
12 int main() {
13     ... foo(1,2);
14     ... return 0;
15 }
16
```

Q 5.1: Assume that execution has reached line 8 (**gets** is being called). Fill in the following stack diagram. Assume that each row represents 4 bytes. Note that arrays are filled from lower addresses to higher addresses and are zero-indexed.

Stack

2
1
RIP of foo
SFP of foo
age
name[8]
name[4]
name[0]

Q 5.2: Assume that the memory address that stores [RIP of **foo**] is 0x12345678.

Construct an input to **gets** that would cause the program to execute malicious shellcode. You may reference **SHELLCODE** as a 12-byte shellcode.

Ans:

SHELLCODE + 'A' * 8 + '\x64\x56\x34\x12'