22/22 Questions Answered
Saved at 2:14 PM

Homework 5

Q1 True/False
4 Points

This homework has instant feedback. When you click "Save Answer," if the answer is correct, you will see an explanation. You can resubmit as many times as you want.

Q1.1
1 Point

Relevant lecture: Thursday, March 18: DNS (slides, Youtube , Kaltura, review videos, notes section 8)

To increase the number of random bits an off-path attacker needs to guess in a DNS query, we often randomize the destination port.

- ○ True
- ◉ False

EXPLANATION

False. We randomize the source port. Destination port is usually fixed for a given service.

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:09 PM**

Q1.2

1 Point

Relevant lecture: Tuesday, March 30: TCP (slides, Youtube , Kaltura, review videos, notes section 6)

An attacker trying to MITM-attack a TCP connection has a better chance of doing so at the beginning of the connection when SYN/ACK sequence numbers are relatively smaller.

- ○ True
- ◉ False

EXPLANATION

False. The initial sequence number is randomly chosen.

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:09 PM**

Q1.3

1 Point

Relevant lecture: Tuesday, March 30: TLS (slides, Youtube, Kaltura, review videos, notes section 7)

Modern implementations of TLS use Diffie-Hellman instead of RSA in the handshake because Diffie-Hellman prevents replay attacks.

- ○ True
- ◉ False

EXPLANATION

False. We use Diffie-Hellman because it provides forward secrecy. (If the server's private key is stolen, past recorded communications cannot be decrypted.) For RSA, the nonces R_b and R_s are used to prevent replay attacks.

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:09 PM**

Q1.4
1 Point

Relevant lecture: Tuesday, March 30: TLS (slides, Youtube, Kaltura, review videos, notes section 7)

There is nothing a man-in-the-middle attacker can do to interfere with a TLS connection.

○ True

◉ False

EXPLANATION

False. For example, an attacker can compromise availability by dropping packets or injecting reset packets.

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:09 PM**

Q2 Packet Reconnaissance
7 Points

Relevant lectures:
Tuesday, March 11: Networking Background (slides, Youtube , Kaltura, review videos, notes section 1)
Tuesday, March 30: TLS (slides, Youtube , Kaltura, review videos, notes section 6)

This question introduces you to some common patterns in networking attacks, such as packet spoofing and the TCP handshake.

The IP packet header has a 16-bit ID field for distinguishing packets. Consider a *patsy server* that implements the ID field by maintaining a single counter that increments by one for every packet it sends,

regardless of the packet's destination. The host sets the ID field in each packet it sends to the current value of the counter.

Suppose this server responds to *ping requests*. If anyone sends the server a ping, the server will send a reply to let the sender know the server is online.

Q2.1

1 Point

EvanBot wants to know if the patsy server has sent a packet to anyone within a certain one-minute window. How many packets does EvanBot need to send to the server to do this?

- ○ 1
- ◉ 2
- ○ More than 2
- ○ EvanBot cannot learn if the server sent a packet

EXPLANATION

EvanBot sends a ping to the server at the start of the one-minute window and another ping at the end of the one-minute window, then checks if the difference in the ID field of the server's responses is greater than 1. If the difference is greater than 1, that must mean the server sent a packet and incremented the counter in the one-minute window.

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:09 PM**

Q2.2

1 Point

EvanBot wants to know if the patsy server has received a packet from anyone within a certain one-minute window. How many packets does EvanBot need to send to the server to do this?

- ○ 1
- ○ 2
- ○ More than 2
- ◉ EvanBot cannot learn if the server received a packet

EXPLANATION

The counter only increments when the server sends a packet, so EvanBot cannot use the method in the previous part to learn whether the server received a packet.

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:10 PM**

Q2.3

1 Point

EvanBot wants to determine whether REGULUS's server is currently accepting TCP connections.

However, Bot wants to conceal its identity from the REGULUS server, so Bot cannot directly send a packet to the REGULUS server. However, this does not stop Bot from sending a *spoofed packet*, where Bot lies about the source IP address of a packet.

Recall the following facts about TCP:

- A host that receives a SYN packet that it is expecting sends back a SYN/ACK response to the source address.
- A host that receives a SYN packet that it is *not* expecting sends back a RST packet to the source address.
- A host that receives a SYN/ACK packet that it is not expecting sends back a RST packet to the source address.
- A host that receives a RST packet sends back no response.

Assume the patsy server from the previous part still exists and is currently inactive (although it will still respond to pings).

What type of packet should EvanBot send to check if REGULUS is accepting TCP connections?

Source IP address:

- ○ EvanBot's IP address
- ◉ The patsy server's IP address
- ○ REGULUS's IP address

EXPLANATION

EvanBot cannot reveal its identity to REGULUS, so the source IP address can't be EvanBot's IP address.

If we spoof a packet from REGULUS, the response will be sent to REGULUS. However, if we spoof a packet from the patsy server, the response will be sent to the patsy server. Although we don't control the patsy server, we can use it to learn some information with the attack in the previous part. See the next parts for the full solution.

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:10 PM**

Q2.4

1 Point

Destination IP address:

- ○ EvanBot's IP address
- ○ The patsy server's IP address
- ◉ REGULUS's IP address

EXPLANATION

Intuitively, we want to send the spoofed packet to REGULUS to check its behavior and see if it's accepting TCP connections.

✔ Correct

Save Answer Last saved on **Apr 07 at 2:10 PM**

Q2.5

1 Point

TCP flag:

- (•) SYN
- ( ) SYN-ACK
- ( ) ACK
- ( ) None

EXPLANATION

The full attack works as follows:

If REGULUS is accepting TCP connections, then it will see a spoofed SYN packet from the patsy server and send a SYN-ACK reply to the patsy server (bullet point 1). The patsy server isn't expecting a SYN-ACK packet, so it will send a RST (bullet point 3).

If REGULUS is not accepting TCP connections, then it will see a spoofed SYN packet from the patsy server and send a RST packet to the patsy server (bullet point 2). The patsy server sees the RST packet and does nothing (bullet point 4).

Finally, EvanBot uses the attack from Q2.1 to learn whether the patsy server sent any messages in this time period. If the patsy server sent a message (counter difference is greater than 1), then REGULUS must be accepting TCP connections. If the patsy server did not send a message (counter difference is 1), then REGULUS must not be accepting TCP connections.

✔ Correct

Save Answer Last saved on **Apr 07 at 2:10 PM**

Q2.6
1 Point

Would this attack still work if the patsy server was active?

- ○ Yes
- ◉ No

EXPLANATION

If the patsy server becomes active, EvanBot can't be sure if the incremented counter is the result of REGULUS sending a SYN-ACK and the patsy server sending a RST, or the patsy server sending a packet to someone else.

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:10 PM**

Q2.7
1 Point

Would this attack still work if the patsy server generated random ID values instead of incrementing a counter?

- ○ Yes
- ◉ No

EXPLANATION

If the ID values are random, EvanBot can no longer learn if the patsy server sent any packets in a given timespan.

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:10 PM**

Q3 TCP

4 Points

Relevant lecture: Tuesday, March 30: TCP (slides, Youtube, Kaltura, review videos, notes section 6)

Bob has just opened his laptop and is attempting to connect to the Internet to visit `www.randomkittengenerator.com`.

Mallory is determined to interfere with Bob's connection. Mallory can leverage off-path, on-path, and man-in-the-middle attacks against Bob, but would prefer to use the easiest attack. Recall that a man-in-the-middle can both observe as well as intercept traffic; an on-path attacker can observe traffic but not intercept it; and an off-path attacker can neither observe nor intercept traffic. Hence, an off-path attack is easier to launch than on-path, and on-path is easier to launch than man-in-the-middle.

For each scenario, which attack will Mallory use (on-path, off-path, or man-in-the-middle)? You may assume that Bob's IP address is known to Mallory.

Q3.1

1 Point

Mallory seeks to create a UDP request to the website's server which appears to come from Bob's IP address. Mallory doesn't need to see the reply.

- (●) Off-path
- ( ) On-path
- ( ) Man-in-the-middle

EXPLANATION

Off-path attack, since she doesn't need to see anything about the server.

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:10 PM**

Q3.2
1 Point

Mallory seeks to create a TCP connection to the website's server which appears to be from Bob's IP address. The server uses the current time to generate the initial sequence number. Mallory doesn't need to see the reply.

- (•) Off-path
- ( ) On-path
- ( ) Man-in-the-middle

EXPLANATION

Off-path attack, since she can predict the initial sequence number.

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:10 PM**

Q3.3
1 Point

Mallory seeks to create a TCP connection to the website's server which appears to be from Bob's IP address. The server uses a secure RNG to generate the initial sequence number. Mallory doesn't need to see the reply.

- ( ) Off-path
- (•) On-path
- ( ) Man-in-the-middle

EXPLANATION

On-path attack, since she can't predict the initial sequence number.

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:11 PM**

Q3.4
1 Point

Mallory seeks to inject content into an existing active TCP connection between Bob and the web server. Mallory knows Bob is paranoid and records his raw traffic, but she does not want him to determine that she has modified the traffic. Assume that Mallory knows the ports involved in the connection.

- ○ Off-path
- ○ On-path
- ◉ Man-in-the-middle

EXPLANATION

A full man-in-the-middle attack, since an on-path attacker can't stop the legitimate response from the server. If Bob sees both Mallory and the legitimate server reply, he will know someone is interfering.

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:11 PM**

Q4 DNS
7 Points

Relevant lecture: Thursday, March 18: DNS (slides, Youtube , Kaltura, review videos, notes section 8)

Alice and hacker Harry are at a cafe. Alice is going to use the cafe wifi to log into her bank account, and Harry wants to steal her password.

Harry knows that the local DNS server lies on the cafe network and is going to try and interfere with its queries. He sends Alice a malicious link that she will click immediately. Clicking the link will redirect her to `bank.com` and cause her computer to generate one DNS query for the bank website.

Q4.1

1 Point

Suppose Harry owns his own website, `harry.com`. He can see any passwords inputted to this site. Harry wants to spoof a DNS response so that when Alice navigates to `bank.com`, she will actually visit `harry.com`, which Harry has configured to look identical to `bank.com`.

What record should Harry include in his spoofed DNS response to achieve this?

Assume the IP address of `www.harry.com` is `6.6.6.6` and the IP address of `bank.com` is `1.2.3.4`.

- ○ `harry.com A 1.2.3.4`
- ○ `harry.com A 6.6.6.6`
- ○ `bank.com A 1.2.3.4`
- ◉ `bank.com A 6.6.6.6`
- ○ `harry.com NS 1.2.3.4`
- ○ `harry.com NS 6.6.6.6`
- ○ `bank.com NS 1.2.3.4`
- ○ `bank.com NS 6.6.6.6`

EXPLANATION

The spoofed record should map the legitimate `bank.com` to the IP address of Harry's malicious website `6.6.6.6`. The record should be type `A` because it maps a name to an IP address. (`NS` records map a DNS zone to a name server.)

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:11 PM**

Q4.2

1 Point

Alice doesn't type in her bank password immediately, but Harry suspects that she will navigate to `bank.com` and type in her password an hour later.

Can Harry use his spoofed response now to steal Alice's password when she enters it an hour later?

- (●) Yes
- ( ) No

If yes, which part of the spoofed DNS response lets Harry achieve this?

- ( ) ID
- ( ) UDP source port
- ( ) UDP destination port
- (●) TTL
- ( ) Harry can't trick Alice an hour from now.

EXPLANATION

Harry can set the spoofed record's TTL (time-to-live) field to a large number so that even though it poisons the cache now, it will remain cached for several hours (or days) and will be used when Alice later navigates to the site.

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:12 PM**

Q4.3

1 Point

Suppose Harry is an on-path attacker. His malware can generate k forged DNS responses that will all arrive before the legitimate response. Assume $k \geq 1$.

What is the probability p that Harry's attack will succeed? (Harry succeeds if Alice accepts any of the spoofed responses as valid.)

- ○ 0
- ○ $\frac{1}{k}$
- ○ $\frac{k}{2^{16}}$
- ○ $\frac{k}{2^{32}}$
- ○ $\frac{k}{2^{64}}$
- ◉ 1

EXPLANATION

Harry can read the contents of the request, so there are no fields to guess. As long as his forged response arrives first, his attack will succeed.

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:12 PM**

Q4.4

1 Point

Now suppose Harry is an off-path attacker. His malware can still generate k forged responses that arrive before the legitimate response.

Assuming the DNS query randomizes only transaction ID, what is the probability p that Harry will succeed?

- ○ 0
- ○ $\frac{1}{k}$
- ◉ $\frac{k}{2^{16}}$
- ○ $\frac{k}{2^{32}}$
- ○ $\frac{k}{2^{64}}$
- ○ 1

EXPLANATION

If only transaction ID is randomized, $p = \frac{k}{2^{16}}$. Harry has k attempts to guess the 16-bit ID, and each attempt succeeds with probability $\frac{1}{2^{16}}$.

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:12 PM**

Q4.5

1 Point

Assuming the DNS query also implements source port randomization, what is the probability p that Harry will succeed?

- ○ 0
- ○ $\frac{1}{k}$
- ○ $\frac{k}{2^{16}}$
- ◉ $\frac{k}{2^{32}}$
- ○ $\frac{k}{2^{64}}$
- ○ 1

EXPLANATION

If source port randomization is added, $p = \frac{k}{2^{32}}$, because Harry must guess the 16 bit ID and the 16 bit source port.

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:12 PM**

Q4.6

2 Points

Harry wants to increase his odds of success by using the Kaminsky attack.

Recall that in the Kaminsky attack, Harry will force Alice to generate m DNS queries for nonexistent domains (e.g. `1.bank.com`, `2.bank.com`, etc.). If Harry can correctly spoof the response to a single one of these queries, he will be able to trick Alice into visiting `harry.com` when she navigates to `bank.com`.

Again, Harry's malware can generate k forged DNS responses **per request** that all arrive before the legitimate response. Assume the DNS query randomizes only transaction ID. What is the probability p that Harry succeeds?

Hint: what is the probability that all of Harry's responses fail on a single request? What is the probability that all of Harry's responses fail on all requests?

- 0
- $1 - (\frac{1}{k})^m$
- $1 - (\frac{k}{2^{16}})^m$
- $1 - (\frac{k}{2^{32}})^m$
- $1 - (1 - \frac{1}{k})^m$
- **$1 - (1 - \frac{k}{2^{16}})^m$**
- $1 - (\frac{1}{m})^k$
- $1 - (\frac{m}{2^{16}})^k$
- $1 - (\frac{m}{2^{32}})^k$
- $1 - (1 - \frac{1}{m})^k$
- $1 - (1 - \frac{m}{2^{16}})^k$
- 1
- None of the above

EXPLANATION

All of Harry's responses fail on a single request with probability $1 - \frac{k}{2^{16}}$.

Since there are m requests, all of Harry's responses fail on all requests with probability $(1 - \frac{k}{2^{16}})^m$.

The probability of success is 1 - (probability that all responses fail on all attempts), which is $1 - (1 - \frac{k}{2^{16}})^m$.

$p = \frac{km}{2^{16}}$ is an acceptable approximation.

✔ **Correct**

Save Answer Last saved on **Apr 07 at 2:13 PM**

Q5 Feedback

0 Points

Optionally, feel free to include feedback. What's something we could do to make the class better? Or, what did you find most difficult or confusing from lectures or the rest of class, and what would you like to see explained better? If you have feedback, submit your comments here.

Your name will not be connected to any feedback you provide. (If you'd like a direct response, please ask over Piazza instead.) Anything you submit here will not affect your grade.

Save Answer Last saved on **Apr 07 at 2:14 PM**

Save All Answers Submit & View Submission >