Q1 Network Security 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: TCP (textbook)

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

Q1.2

1 Point

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

○ True

● False

Q1.3
1 Point

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

○ True

● False

Q1.4
1 Point

Relevant lecture: DNS (textbook)
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

Q2 Packet Reconnaissance

7 Points

Relevant lectures:
Relevant lecture: TCP (textbook, slides, recording)

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

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

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

Q2.4
1 Point

Destination IP address:

○ EvanBot's IP address

○ The patsy server's IP address

● REGULUS's IP address

Q2.5
1 Point

TCP flag:

● SYN

○ SYN-ACK

○ ACK

○ None

Q2.6
1 Point

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

○ Yes

● No

Q2.7
1 Point

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

○ Yes

● No

Q3 TCP

4 Points

Relevant lecture: TCP (textbook)

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

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

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

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

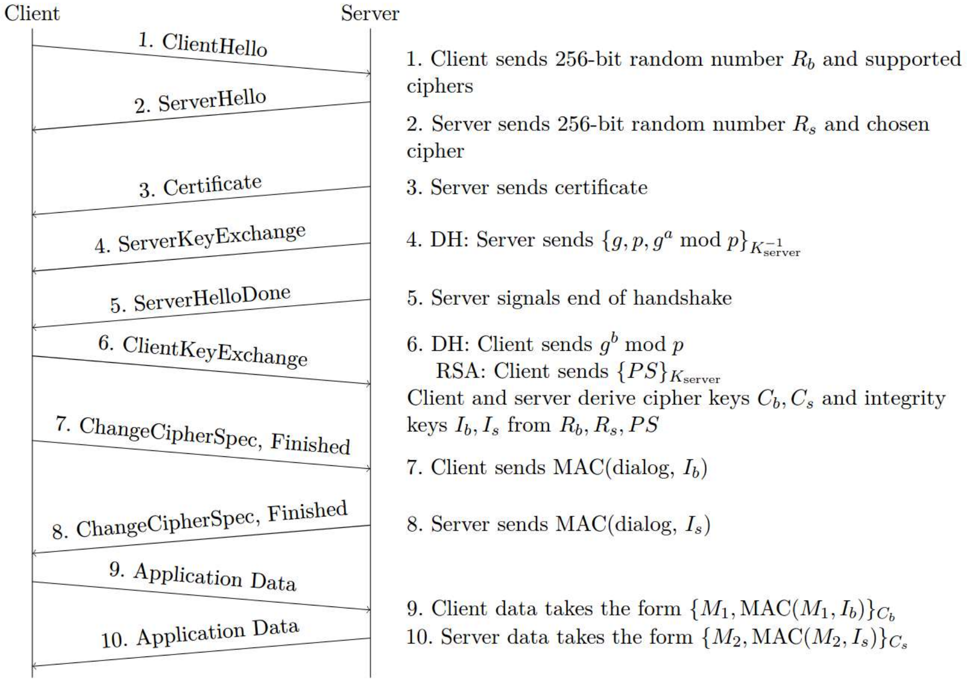
● Man-in-the-middle

Q4 TLS

5 Points

Relevant lecture: TLS (textbook)

This diagram of the TLS handshake from might be helpful to reference throughout the question:



1. Client sends 256-bit random number R_b and supported ciphers

2. Server sends 256-bit random number R_s and chosen cipher

3. Server sends certificate

4. DH: Server sends $\{g, p, g^a \bmod p\}_{K_{\text{server}}^{-1}}$

5. Server signals end of handshake

6. DH: Client sends $g^b \bmod p$
   RSA: Client sends $\{PS\}_{K_{\text{server}}}$
Client and server derive cipher keys C_b, C_s and integrity keys I_b, I_s from R_b, R_s, PS

7. Client sends MAC(dialog, I_b)

8. Server sends MAC(dialog, I_s)

9. Client data takes the form $\{M_1, \text{MAC}(M_1, I_b)\}_{C_b}$
10. Server data takes the form $\{M_2, \text{MAC}(M_2, I_s)\}_{C_s}$

Q4.1

1 Point

Suppose that in TLS with RSA, in Step 1, the client always sends a public constant R_b, and in Step 2, the server always sends a public constant R_s. How does this affect the security of TLS?

○ An on-path attacker can learn all the symmetric cipher keys and integrity keys.

● An on-path attacker can perform a replay attack.

○ An on-path attacker cannot learn the symmetric keys or perform a replay attack.

Q4.2
1 Point

Suppose that in TLS with RSA, in Step 1, the client sends a public constant R_b. (The server sends random R_s as normal in Step 2.) How does this affect the security of TLS?

○ An on-path attacker can learn all the symmetric cipher keys and integrity keys.

○ An on-path attacker can perform a replay attack.

● An on-path attacker cannot learn the symmetric keys or perform a replay attack.

Q4.3
1 Point

Suppose that in TLS with RSA, in Step 6, the client uses the current time, with millisecond precision, as the pre-master secret. How does this affect the security of TLS?

● An on-path attacker can learn all the symmetric cipher keys and integrity keys.

○ An on-path attacker can perform a replay attack.

○ An on-path attacker cannot learn the symmetric keys or perform a replay attack.

Q4.4
1 Point

Modern versions of TLS only support generating the pre-master secret with Diffie-Hellman. Why do we no longer support TLS with RSA?

○ Diffie-Hellman is faster than RSA

○ Pre-master secrets generated from Diffie-Hellman are harder to brute-force than pre-master secrets generated from RSA

● Diffie-Hellman keeps a communication secure even if someone compromises the keys later, while RSA does not

Q4.5
1 Point

Suppose that in TLS with Diffie-Hellman, in Step 4, the server does not send a signature along with $g, p, g^a \bmod p$. How does this affect the security of TLS?

○ A MITM attacker can learn all the symmetric cipher keys and integrity keys.

○ A MITM attacker can perform a replay attack.

● A MITM attacker can impersonate the server.

○ A MITM attacker cannot do any of the above.

Q5 DNS
6 Points

Relevant lecture: DNS

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.

Q5.1
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`

Q5.2
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.

Q5.3
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

Q5.4
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

Q5.5
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

Q5.6
1 Point

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

Q6 Project 3 (Web Security) Warmup

8 Points

In Project 3, you will be finding web security vulnerabilities in a poorly-designed website. This question will walk you through some strategies for analyzing a website for security flaws.

We recommend using Firefox or Chrome for this question (and for Project 3).

Q6.1

1 Point

Relevant lecture: Intro to Web (textbook)

First, visit https://cs161.org/hw6 in your favorite browser. Examine the HTML for this page by right-clicking and choosing "View page source."

There is a secret hidden as an HTML comment. Enter the secret below.

bobbytables

Q6.2

1 Point

Next, let's look at the HTML form. If you click "Submit," what type of HTTP request does this form send?

(The CS161 website can't generate custom responses to requests, so if you click Submit, you'll be sent to https://postman-echo.com, a dummy endpoint.)

○ HTTP GET

● HTTP POST

Q6.3
1 Point

Relevant lecture: CSRF (textbook)

This form implements CSRF protection using CSRF tokens. Assume that these tokens are high-entropy and randomly generated by the server each time.

```
<input type="hidden" name="csrf-token" value="5f4dcc3b5aa765d61d8327deb882cf99">
```

Is this a good defense against CSRF attacks?

● Yes, because an attacker cannot guess the CSRF token value

○ Yes, because the `type=hidden` attribute means an attacker cannot see the CSRF token value

○ No, because the attacker can view the page source and see the CSRF token value

○ No, because CSRF tokens are a weak defense against CSRF attacks

Q6.4
1 Point

Now, go back to https://cs161.org/hw6. Right-click and select "Inspect element" (Firefox) or "Inspect" (Chrome). You should see a panel appear with the HTML source of the page.

In the HTML, find the line `<a href="https://cs161.org">CS161 Home page</a>`. (You can use Ctrl+F in the Inspect panel if you're having trouble finding this line.)

Right-click this line of text and select "Edit as HTML." Change the link to `https://cs161.org/phishing`.

Now try clicking the link on the page. You've phished yourself!

If another student loads this website in another browser and clicks on the link, will they fall victim to your phishing attack?

○ Yes, because the HTML has been changed to link to the phishing page.

○ Yes, because the website has not implemented XSS protection.

● No, because you have not changed the server-side HTML.

○ No, because the website has implemented XSS protection.

Q6.5
1 Point

Relevant lecture: Cookies and Session Management (textbook)

Next, let's see how to view cookies.

In the Inspect Element panel, choose the "Storage" (Firefox) or "Application" (Chrome) tab.

How many cookies are set on this webpage?

○ 1

○ 2

● 3

○ 4

Q6.6
1 Point

Find the cookie with `Name=session`.

What is the value of the cookie?

● 1612020

○ yes

○ warmup

○ tracking

○ .cs161.org

Q6.7
1 Point

If you load the page https://cs161.org/calendar, will the cookie with `name=session` be sent to the server?

● Yes

○ No

Q6.8
1 Point

If you load the page http://cs161.org/hw6, will the cookie with `name=session` be sent to the server? (Ignore any redirection for this question.)

○ Yes

● No

Q7 Feedback

0 Points

Optionally, feel free to include feedback. Any TA's you like to shout out? 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.

Homework 6

● Graded

Select each question to review feedback and grading details.

Student

Yiyun Chen

Total Points

34 / 34 pts

Question 1

Network Security True/False	**4** / 4 pts
1.1 (no title)	**1** / 1 pt
1.2 (no title)	**1** / 1 pt
1.3 (no title)	**1** / 1 pt
1.4 (no title)	**1** / 1 pt

Question 2

Packet Reconnaissance	**7** / 7 pts
2.1 (no title)	**1** / 1 pt
2.2 (no title)	**1** / 1 pt
2.3 (no title)	**1** / 1 pt
2.4 (no title)	**1** / 1 pt
2.5 (no title)	**1** / 1 pt
2.6 (no title)	**1** / 1 pt
2.7 (no title)	**1** / 1 pt

Question 3

TCP	**4** / 4 pts
3.1 (no title)	**1** / 1 pt
3.2 (no title)	**1** / 1 pt
3.3 (no title)	**1** / 1 pt
3.4 (no title)	**1** / 1 pt

Question 4

TLS	**5** / 5 pts
4.1 (no title)	**1** / 1 pt
4.2 (no title)	**1** / 1 pt
4.3 (no title)	**1** / 1 pt
4.4 (no title)	**1** / 1 pt
4.5 (no title)	**1** / 1 pt

Question 5

DNS		**6** / 6 pts
5.1	(no title)	**1** / 1 pt
5.2	(no title)	**1** / 1 pt
5.3	(no title)	**1** / 1 pt
5.4	(no title)	**1** / 1 pt
5.5	(no title)	**1** / 1 pt
5.6	(no title)	**1** / 1 pt

Question 6

Project 3 (Web Security) Warmup		**8** / 8 pts
6.1	(no title)	**1** / 1 pt
6.2	(no title)	**1** / 1 pt
6.3	(no title)	**1** / 1 pt
6.4	(no title)	**1** / 1 pt
6.5	(no title)	**1** / 1 pt
6.6	(no title)	**1** / 1 pt
6.7	(no title)	**1** / 1 pt
6.8	(no title)	**1** / 1 pt

Question 7

Feedback	**0** / 0 pts