ECE 458/750: Computer Security Final			Marks obtained ↓
Date: Aug 15, 2024,	Total questions: **12**	Total points: **66**	
ID:	Name:		Time: 2.5 hrs

Instructions

No aids allowed. All you are allowed is a pen and pencil.

Use space provided. Answer the questions in the spaces provided. If you run out of room for an answer extra pages are provided at the end of the test booklet starting on page 15. They are clearly marked as EXTRA ANSWER SPACE. Please state in the original answer space if the extra pages are being used so that the grader knows to look there.

Point value in right-hand margin. The number of points each question is worth is listed in the right hand margin. The number of points and the space provided are roughly indicative of how long of an answer is expected.

Pencils and pens allowed. Both pens and pencils are allowed. Pencil marks need to be clearly present or erased. If it is unclear if a mark is or is not present then it is up to the discretion of the grader and this point cannot be contested later.

General Security Questions

1. In the definition of security, what do the letters CIA stand for? Fill in the blanks below. (3)
   C _____
   I _____
   A _____

   Solution: Confidentiality, Integrity, Availability.

2. Which of the following best describes the purpose of the Federal Trade Commission (FTC) in the US which is similar to the Office of the Privacy Commissioner (OPC) of Canada. Tick or circle the best answer. (2)

   ◯ Ensure that company privacy policies are in alignment with their practices
   ◯ Help consumers make good decisions around selecting companies to engage with
   ◯ Regulate industry to protect consumers from unfair or deceptive trade practice
   ◯ Provide consultancy services to help companies proactively setup good privacy and trade practices

   Solution: Regulate industry to protect consumers from unfair or deceptive trade practice

3. If you were to enter the following URL into a browser what website would the browser attempt to visit? (Note the URL is fake and will result in an error, but the browser will still attempt to visit a site.) (2)

   https://twitter.com@facebook.vpn.com/safesite.com/index.html

   ◯ Twitter
   ◯ Facebook
   ◯ VPN
   ◯ Safesite

   Solution: VPN. The twitter.com is in the username position and will be ignored. Facebook is a subdomain. Safesite is a subdirectory. VPN is in the domain position so the browser will attempt to visit it and then ask it where to find the subdomain "Facebook".

4. Modern websites are constructed from many different sources. For each of the following statements, indicate if the statement is True or False. Assume that technology is working as expected and no vulnerabilities are being exploited. (4)

   _____ Content loaded from third parties can in turn cause more content to load.

   _____ Operating system version information is sent with every web request.

_____ The General Data Protection Regulation (GDPR) requires consent to be obtained every time a user's IP address is sent to third parties.

_____ Popular browsers like Chrome and Firefox allow website owners to write and read files from the user's computer without explicit approval.

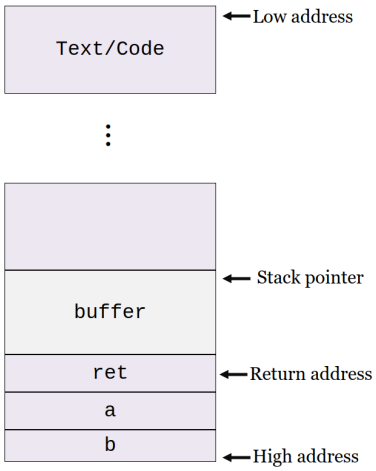
Solution: True, True, False, False

5. If a password is stored hashed but no salt is used what kind of offline attack becomes possible? (4)

Solution: A rainbow table attack. An attacker can pre-compute the password hashes of a large dictionary of previously-used passwords. Then each hashed password is an O(1) lookup in the table to obtain the matching plaintext. If a suitably large salt is used, then pre-computing is not possible and each password requires O(N) guesses to find the correct password where N is the size of the set of possible passwords.

Buffer Overflow

6. The following picture depicts a stack-smashing buffer overflow. The stack grows "downwards," while the buffer is written "upwards". The contents of the buffer therefore "smash" the stack. (10)



Describe one mitigation strategy that an operating system can use to prevent the stack from being smashed. Briefly explain how the mitigation is implemented and why it prevents stack smashing.

Solution: Canary is the most obvious answer. A canary is a set of bits that are written write below the return address. Ideally the canary also includes characters like the null termination character used to end strings. If a buffer overflow happens then the canary is also written over allowing the operating system to detect the problem and safely terminate.

QUESTION 6 ANSWER SPACE

Cryptography

7. Off-The-Record Messaging is a protocol designed to provide Repudiation (R from STRIDE). After every conversation the keys require to encrypt messages are published publicly while the keys required to decrypt the messages are deleted. Explain how publishing the encryption keys and allowing Repudiation improves privacy? (6)

Solution: Repudiation means that it is unclear or impossible to prove who performed an action. In this case, it means that it is impossible to prove who encrypted a message. In theory, if Alice and Bob communicated using Off-The-Record Messaging and an attacker Eve recorded their messages, even if the attacker was able to find some way to decrypt the messages, they could never prove that Alice or Bob sent them. Because everyone has the encryption key. So everyone has the ability to create new encrypted chats, including Eve.

8. The authenticity security property in a protocol guarantees that each party in the protocol is who they claim to be. For the two approaches below, state what would need to be true in order to use them while maintaining authenticity. (6)

   (a) Hash-based Message Authentication Code (HMAC)

   (b) Asymmetric cryptography

> **Solution:** HMAC is Suitable for scenarios where both parties share a secret key. They must have the same key and no one else may have the key.
>
> Asymmetric cryptography means the users have different keys. To maintain authenticity, they need some way to verify the owner of the other key. They also need to ensure that no one else has that key.

Networking

9. In class we learned about Network Address Translation (NAT) devices and Virtual Private Networks (VPN) servers. Both technologies alter the source and destination IP addresses of traffic flowing across them.

   (a) The definition of security involves five properties known as CIAAA. Name two of the properties that a VPN can provide but a NAT cannot and a very brief description of how it provides them. Simple descriptions featuring keywords are encouraged. (4)

   > **Solution:** Confidentiality and Integrity. A NAT does not provide encryption and a VPN does. Encryption provides Confidentiality by hiding the content of data in transit. It also provides Integrity by ensuring data is not changed in transit.
   >
   > Authentication is also an appropriate answer if well justified. A VPN should be using a public/private key pair that the VPN client is able to validate. The VPN may also require the user to be registered and log into it, so the VPN may also do some authentication of the user. So there is some Authentication security in terms of sending data to the VPN server, but not past that point.

   (b) Man In The Middle (MITM) attacks can happen when using a VPN. Describe a situation where the VPN is operating correctly yet a MITM attack where the attacker can see and modify traffic still happens. (6)

   > **Solution:** A VPN protects network traffic between the client and the VPN, it does not protect traffic between the VPN and the end destination. If traffic is sent unencrypted (i.e. http from a browser) then it can be MITM attacked between the VPN server and the destination.

QUESTION 9 ANSWER SPACE

10. Onion routing, of which Tor is an example, provides further privacy protections in addition to what a typical VPN provides. Joseph wants additional privacy so he decides to route all the traffic from his computer across the Tor network. Explain why doing so is dangerous and is likely to result in less privacy. (5)

Solution: Onion routing improves privacy in terms of anonymity of the original IP address. It makes sure that no one knows the original IP address of the sender of a packet. However, Tor exit nodes are run by volunteers world wide. Traffic exiting a Tor node is quite likely to be captured, scanned, and possibly modified if it is not properly protected by encryption. When downloading Tor it typically comes with a bundled browser that is setup to make sure https is being used (among other things).

The problem with Joseph sending all his computer traffic through Tor is that there is no guarantee that it is all encrypted. Many applications and programs do a poor job encrypting traffic or don't encrypt it at all. Some of the Tor exit nodes he will be assigned are likely to be hostile, such as a foreign government trying to get information about another nation's citizens. If even one application on Joseph's computer is not encrypting traffic and has a vulnerability, then the Tor exit node can perform a Man-in-the-Middle attack, inject attack code, and gain some access to Joseph's computer which completely negates any privacy improvement Joseph may have gotten from using Tor.

The other problem is that Tor's protections are only useful if the user is anonymous to the service they are accessing. Many apps and applications on a computer send unique codes to their servers that identify the user. In such a case, Joseph would not get any benefit from using Tor since the traffic itself leaks his identity. It would also possibly allow an attacker with visibility of what is going in and out of the Tor exit node Joseph is using to see what other sites are being contacted and link those sites with Joseph. In other words, sending all the traffic, including traffic with identifiers, can leak information and increase the odds of being identified compared to only using Tor for a limited set of traffic.

Web Security

11. Figure 2 (next page) shows a simple webpage and Figure 1 shows the HTML/JavaScript code for the page. The user is attempting to pay the bank using a credit card but the bank only accepts Mastercard and they would like to use a Visa card. Thankfully for the user, the bank has made a security mistake in the design of their page. (10)

```
<HTML>
<HEAD>
<script>
cardNumberOK = false;

function checkCard(){
  ccnum = document.getElementById('ccnum').value;

  // Mastercard numbers start with a 5
  if(Array.from(ccnum)[0] == 5){
    cardNumberOK = true;
    submitToServer();
  } else {
    alert("Error: we only accept Mastercard!");
  }
}

function submitToServer(){
  // Code that reads the form information and if cardNumberOK==true,
  // sends the information to the server
}
</script>
</HEAD>

<BODY>
<H1>Bank</H1>
To pay off your credit card bill, enter your card number and name
below. Note that we only accept Mastercard.<BR><BR>

 <form >
  <label>Card Number:</label>
  <input type="text" id="ccnum"><br><br>
  <label>First name:</label>
  <input type="text" id="lname"><br><br>
  <label>Last name:</label>
  <input type="text" id="lname"><br><br>
  <button onclick="checkCard()">Submit</button>
</form>

</BODY>
</HTML>
```

Figure 1: HTML and JavaScript for a bank website that takes credit card details from the user and sends them to a server.

(a) Explain the security issue that the website in Figure 1 has. The issue is an example of a wider class of security flaws, state the name of or clearly explain the wider flaw type.

Solution: The website looks like it has *Incomplete Mediation* which means that they are checking a fact (card type) on one side of a trust boundary, but possibly not checking it on the

server. In this case line 10 checks if the card number starts with a 5 and then sets a global variable. But the rest of the code just trusts the global variable, particularly submitToServer() on line 18. Its impossible to know what the server will do, but a skilled penetration tester would send in a number that does not start with 5 to see what happens.

(b) Explain the steps you might take to exploit the error and successfully pay using a Visa card.

Solution: The website is checking the card number client-side. It is impossible to know what the server is doing but there is a good chance that the server may trust the client-side check. If so, it should be possible to pay with a Visa by entering a Visa card number and then either: 1) setting cardNumberOK to true and calling submitToServer() directly, or 2) modifying the if in checkCard() to not check. Because this code is running on the client, the user can modify it or even execute JavaScript commands directly.

Solution: POST MARKING NOTES for question 11 a and b.

- Possible attack without modifying the Javascript: enter "5" for the credit card and click submit. This will set cardNumberOK to true but not pay anything because 5 is not a valid credit card. Then enter real card and call submitToServer() directly.
- There is also a potential race condition here since the check happens, and then submitToServer then fetches the text value from the input box again. Best answer I saw that did not involve id not involve editing JavaScript directly (better answer).
- BufferOverflow is not possible to do client-side in this case. First off JavaScript is an interpreted language so it does not impact the stack directly and cannot perform a stack smash. Second, attacking the client is not helpful to the situation. The user already has strong control over the client.
- Adding a "¡script¿" tag to the input boxes will not solve the problem. Lines XX-xx have unknown code, so it is possible that strings are being joined without escaping characters. But having unexcaped script statements in the middle of a string concatination isn't going to cause code to be executed. XSS works by having one computer (server) give unexscaped code to another computer (client) who executes it. Creating the code on one computer alone won't work, it will just produce an error.

QUESTION 11 ANSWER SPACE

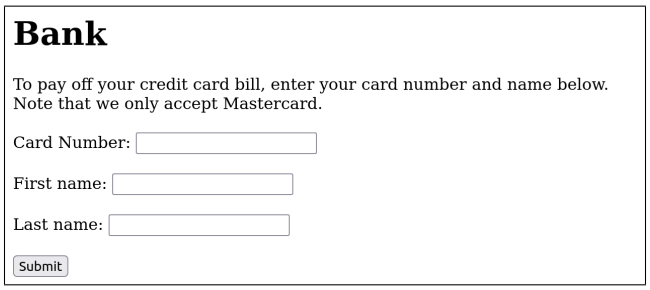


Figure 2: Bank website to take payment information.

QUESTION 11 ANSWER SPACE

12. Describe how a session cookie is different from other types of web cookies in terms of: i) how it is technically implemented, and ii) privacy implications. (4)

Solution:

i) Session cookies are identical to normal cookies. There is no technical difference. A session cookie just has a short expiration time or there is no expiration time. Most browsers (not Firefox) will delete cookies without an expiration whenever the browser is closed. So cookies without an expiration are expected to be automatically deleted fairly regularly.

ii) Session cookies are used to solve the technical problem of internet state and are used to track a single session between the client and the server. Because the session is not considered to be a privacy issue, tracking it is not problematic. GDPR, for example, considers session cookies to be Legitimate Interest when they are being used for session maintenance. It is cross session tracking that is normally considered to be a privacy problem.

Extra Answer Space

If you need extra space to give an answer, please state in the original answer space that you will be using the extra pages and continue or write your answer here.

EXTRA ANSWER SPACE

EXTRA ANSWER SPACE