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 13. 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 _____

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

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

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.

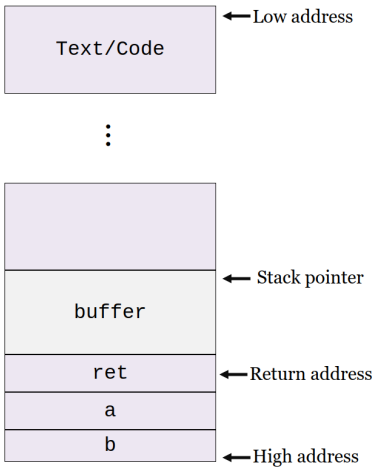
   _____ The General Data Protection Regulation (GDPR) requires consent to be obtained every time a user's IP address is sent to third parties.

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

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

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.

QUESTION 6 ANSWER SPACE

Cryptography

covered more in 2024

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)

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

Networking

Not covered in 2025

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)

   (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)

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)

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.

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

QUESTION 11 ANSWER SPACE

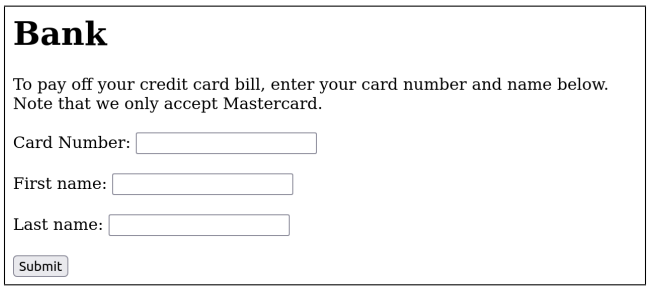


Figure 2: Bank website to take payment information.

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)

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