**COMP435 WA6** Name: _____

**Question 1: CSFR Attack** A cross-site request forgery (CSRF) is an example of a confused deputy attack. Answer the following questions with respect to a CSRF attack.

1.1. Which entity in the CSRF attack is the deputy?

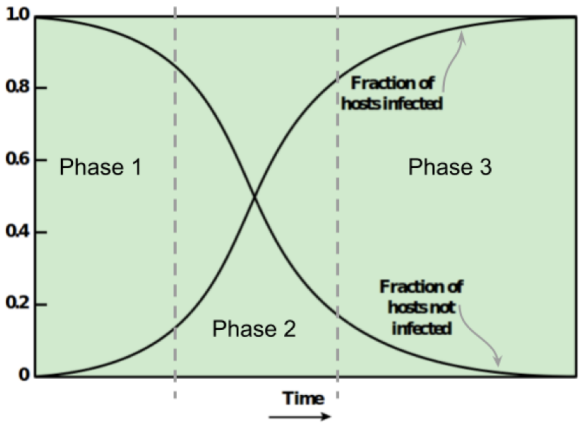
1.2. Which authority does the deputy use indiscriminately?

1.3. What is an access control mechanism for stopping confused deputy attacks?

**Question 2: Virus Infection Strategies** Two virus infection strategies are overwriting at the interior of the target host file or appending to the end of the target host file.

2.1. What is one reason an attacker might choose the "overwriting at the interior" strategy?

2.2. What is one reason the attacker might choose the "appending to the end" strategy?



Computer Security: Principles and Practice, 3rd Ed. Stallings and Brown

**Question 3: Worm Propagation** The figure above shows a plot of the saturation of a worm in a network as time progresses. The plot is divided into three phases.

3.1. In which phase is the number of new machines infected increasing exponentially?

3.2. Using the same figure, in which phase is a worm most likely to use permutation scanning as a strategy to find new machines to infect and why?

**Question 4: Straight A's for All!** The leader of the student-led campus organization "Straight As for All" wants to attract attention to their cause and is willing to break the law to do so. Which type of malware are they more likely to deploy, a worm or a rootkit, and why?

```
query = "SELECT * FROM pswdtab
WHERE username='" + name + "'
AND password='" + passwd + "'"
```

**Question 5: SQL Injection Attack** A web server takes in a username and password from a user, uses those values to formulate a SQL query, and passes along the SQL query to the database server. The following figure shows how the SQL query is formulated by the web server.

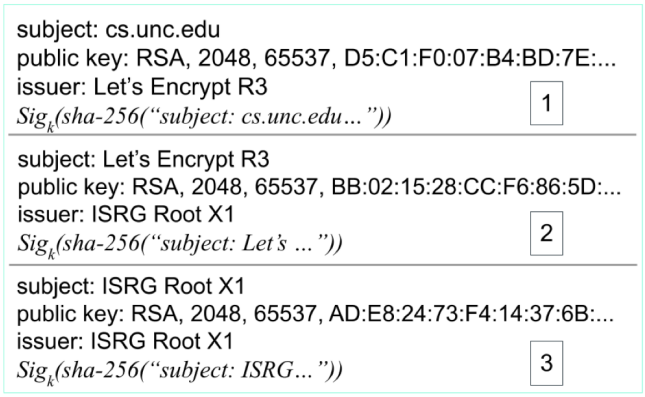
If the user submits the name: `Robert'; DROP TABLE pswdtab --` and the password: `1234567...`

5.1. What will be the exact query that gets sent to the database server?

5.2. What actions will be taken by the database server in response to this query?

5.3. What would happen if the user submitted the text none in the password field? Explain why.

**Question 6: Dolev-Yao Attacker Model** Name two powers that the attacker is assumed to have in the Dolev-Yao model for network security.




**Question 7: Certificate Chains** The following figure depicts a certificate chain presented to a browser.

7.1. Which key is used to create the signature in certificate (1)? Be specific.

7.2. In order to verify this certificate chain, the browser must already know:

- ◯ the browser needs no additional information
- ◯ cs.unc.edu's private key
- ◯ ISRG Root X1's private key
- ◯ ISRG Root X1's public key
- ◯ Let's Encrypt R3's public key

7.3. Who is the trust anchor in this chain? How can you tell?

**Question 8: More Certificates** Alice is browsing the web and clicks on a link taking her to the site https://amazon.money.com. She notes the lock icon in the URL bar of her browser and sees that the page looks like the usual landing page for Amazon.

8.1. Alice can be confident that she is securely visiting the Amazon site. (True/False and Why)

8.2. Alice clicks the lock icon in her browser's URL bar to check the certificate and sees that it is a valid certificate issued to amazon.money.com by Let's Encrypt with the root certificate authority ISRG Root X1. With this information, Alice can be confident that she is:

- ◯ at a legitimate (non-malicious) website
- ◯ securely logged-in to the Amazon website
- ◯ communicating over an encrypted TLS channel

8.3. Alice logs in using her Amazon username and password and sees the expected "Hello, Alice" message. She puts a few things in her cart and checks out as usual. She notices that the site seems a bit slow, but otherwise everything is as expected. The next day her Amazon packages arrive. The day after that she sees unexpected charges on her credit card; her credit card information has been stolen. Explain what likely happened.

**Question 9: Public Key Infrastructure** What is the main goal of public key infrastructure? Respond with a one concise sentence.