Cybersecurity Cryptography Homework

A. From a service perspective, what is an important difference between a symmetric-key system and a public-key system?

- In symmetric-key, both the sender and the recipient share a secret key. In a public key system, a public key is available to everyone, while only the receiver knows the private key.

B. Can you "decrypt" a hash of a message to get the original message? Explain your answer

- No you cannot, by design a hash has no inverse.

C. Consider a variation of the MAC algorithm where the sender sends (m, H(m) + s), where m is the message and H(m) + s is the concatenation of H(m) and s, which is the secret key. Is this variation flawed? Why or why not?

- Yes this method is flawed. THe intruder can hash H(m) and extract "s". The extraction is (H(m) + s - H(m)).

D. Suppose certifier.com creates a certificate for foo.com. Typically, the entire certificate would be encrypted with certifier.com's public key. True or False?

- False, it should be encrypted with the private key, not public. Also only the information's digital fingerprint is encrypted by the certifier's private key.

E. In the SSL record, there is a field for SSL sequence numbers. True or False?

- False.

F. Consider the polyalphabetic system shown below. Will a chosen plaintext attack that is able to get the plaintext encoding of the message "The quick brown fox jumps over the lazy dog." be sufficient to decode all messages? Why or why not

- Yes this will be enough. That sentence contains every letter of the alphabet so each letter can be decoded.

G. What is the difference and similarity of MAC and a digital signature?

- Mac uses symmetric keys and is used within a message in blocks. A digital signature uses a private key which is decrypted with a public key. Also it is used to validate the whole message.

H. Provide a detailed diagram of how the CA public key and the server's public key are used in SSL.

- A website registers its public key for the domain "example.com" with CA.
- CA creates certificate binding example to its public key.
- The cert contains the server's public key digitally signed by CA.

I. Extending the last question, list all the steps from the company that owns the server getting the public key certificate to the client getting the public key from the server. Now, list two possible security vulnerabilities and indicate how likely the vulnerability could be exploited.

- The root public key is added to the OS, browser, etc.
- The CA generates a set of intermediate public and private keys.
- These keys are signed with the CA's root private key. CA uses its intermediate key to sign and generates 2 certs.
- The cert proves the CA public key is correct.

- A cert that signs the example’s public key is signed with the intermediate private key.
- When a browser gets the cert from the example, it gets 2 certs. One signs the CA’s intermediate public key, and one that signs the example’s public key.

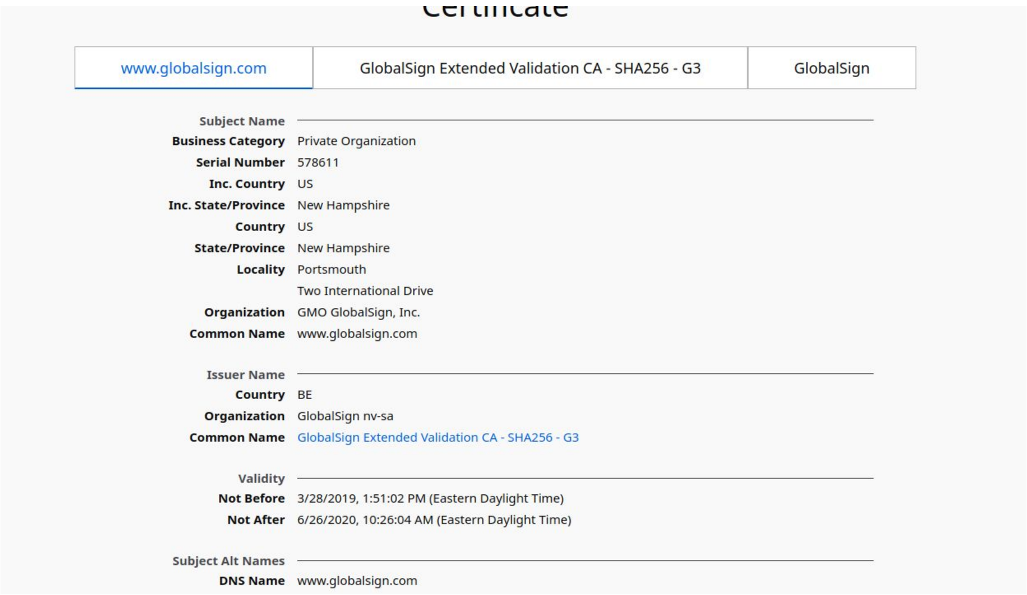
- One vulnerability is the ability to perform a man in the middle attack. A website’s server key could be stolen, allowing the attacker to appear as the server. This is one of the most likely ways to exploit, as there are many ways to pretend to be one of the two parties communicating.

- Another vulnerability is the use of “wildcard” certificates. These are self-signed certificates, which erodes trust because no third-party CA ever verifies these certs. This is likely to happen without proper rules in place to stop admins from creating these wildcard certs.

J. In SSL, why is symmetric key encryption used when public key encryption is also used. Could public keys be used without symmetric key? If so, why is symmetric used.

- Server sends a copy of its asymmetric public key, Browser creates a symmetric session key and encrypts it with the server's asymmetric public key. Then sends it to the server. Thus server and browser now encrypt and decrypt all transmitted data with the symmetric session key. This allows for a secure channel because only the browser and the server know the symmetric session key, and the session key is only used for that session. If the browser was to connect to the same server the next day, a new session key would be created
- Public keys could be used with symmetric, but symmetric is used to hide the key from the outside world.

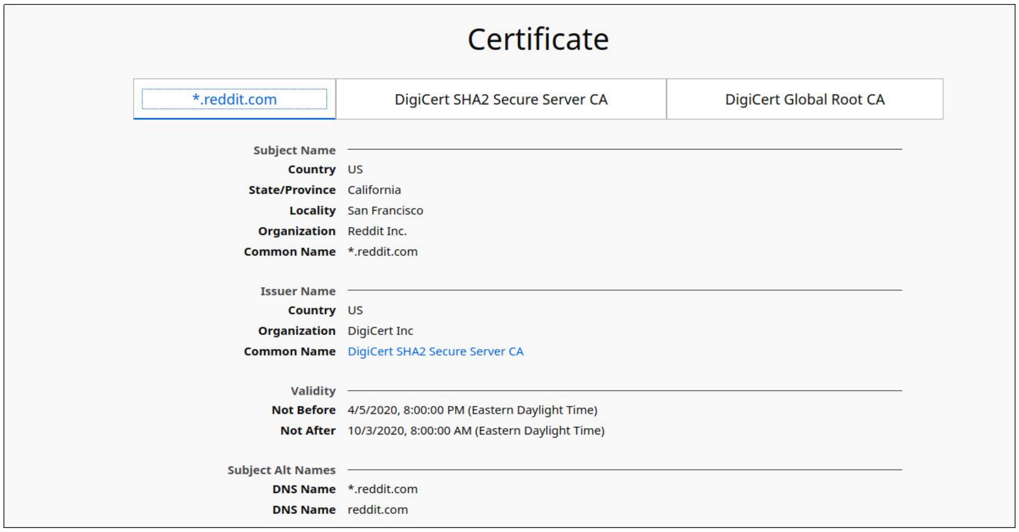
K. Use the certificate explorer in chrome to view an SSL certification. Generate screen shots that show the certificate path and the expiration date. Find examples where the Subject field shows that only specific URLs are signed (like www.example.com) and an example when an entire domain is signed (like *.example.com)



Certificate

www.globalsign.com | GlobalSign Extended Validation CA - SHA256 - G3 | GlobalSign

Subject Name	
Business Category	Private Organization
Serial Number	578611
Inc. Country	US
Inc. State/Province	New Hampshire
Country	US
State/Province	New Hampshire
Locality	Portsmouth
	Two International Drive
Organization	GMO GlobalSign, Inc.
Common Name	www.globalsign.com
Issuer Name	
Country	BE
Organization	GlobalSign nv-sa
Common Name	GlobalSign Extended Validation CA - SHA256 - G3
Validity	
Not Before	3/28/2019, 1:51:02 PM (Eastern Daylight Time)
Not After	6/26/2020, 10:26:04 AM (Eastern Daylight Time)
Subject Alt Names	
DNS Name	www.globalsign.com



Certificate

*.reddit.com | DigiCert SHA2 Secure Server CA | DigiCert Global Root CA

Subject Name	
Country	US
State/Province	California
Locality	San Francisco
Organization	Reddit Inc.
Common Name	*.reddit.com
Issuer Name	
Country	US
Organization	DigiCert Inc
Common Name	DigiCert SHA2 Secure Server CA
Validity	
Not Before	4/5/2020, 8:00:00 PM (Eastern Daylight Time)
Not After	10/3/2020, 8:00:00 AM (Eastern Daylight Time)
Subject Alt Names	
DNS Name	*.reddit.com
DNS Name	reddit.com

L. Installing fake certificate authority public keys (see https://udel.instructure.com/courses/1498333/files/84167431/download)

a. Suppose a hacker installs a new certificate authority public key on a computer, what will that allow?

- It will allow unauthorized requests in the computer, because the computer will tell that it is safe to do certain actions as the request is from a safe sender(which is actually dangerous but as the hacker has modified the checking system of certificate with will validate the request accordingly and allow the request).

b. Now suppose that a company installs their own certificate authority public key on an employee laptop. Why would a company install its own certificate authority public key on employee machines?

- To make sure that the only authorised requests are made to the employee's laptop whose certificates are trusted by the company the company will install their own certificate authority public key on an employee laptop.

c. What are the security threats of a company installing a CA public key on employee laptops?

- If the employee's laptop security is compromised or the employee itself leaks the CA public key then the outside person can make the certificates just according to the criteria of CA and can make their requests validated and steal the data.

M. Covid-19 contact tracing:

a. Option 1. Each phone broadcasts the phone's phone number. All nearby phones receive those numbers and the time when the number was received. If someone gets sick, all saved phone number are called. Why is this a privacy risk

- This is a privacy risk because the someone who previously didn't know/did not have access to a phone number can possibly access it when it is saved or called. It's possible to now know the authenticity of the phone number's that are being broadcasted.

b. Option 2. Each phone has the health department's public key and broadcast's its phone number encrypted via the health department's public key. Each phone records the encrypted phone numbers of the nearby phones and the time when received.

i. What happens when someone is found to be sick?

- All nearby phones receive the encrypted phone number of each phone. The number is encrypted with the public key.

ii. Does this option solve the privacy issues that the first option suffers from?

- Yes, because we know that the phone number being sent and encrypted is legitimate because it has been "sealed" with the public key.

iii. Are there other privacy issues?

- Yes, it is possible that a replay attack is used.

iv. Should a nonce be used to improve privacy?

- Yes, if a nonce is used then a replay attack could be detected. The nonce value would show an attack because the nonce value of the attack doesn't match the current nonce value.

N. My browser sometimes shows the text https crossed out and an “x” on a lock symbol. What does this mean? Is there a security risk? If so, explain how the vulnerability could be exploited.

- This means that the identity of the website has not been verified and the server’s certificate does not match the URL. It is possible that it’s partially encrypted or it’s encrypted with a party that is not trusted. This is a security risk because if it’s partially encrypted, the data can be sniffed on a network. It’s also possible that you’ve gone to an imposter website like “gooogle.com” instead of “google.com” and the data is then being sent to an attacker.