CMPT 403: Written Assignment 2

Vaibhav Saini – 301386847

Question 1

(a) The mistake in this scenario is that Alice is using RSA encryption to directly encrypt a 128-bit secret key intended for AES in CBC mode and then using a SHA-256 HMAC with the same key to authenticate the message.

Instead, Alice should generate a random 128-bit secret key for AES in CBC mode and encrypt the secret key using Bob's RSA public key. Then, she should use a secure key derivation function, such as PBKDF2 or bcrypt, to derive a cryptographic key from the shared secret key. This derived key can be used for AES encryption. Additionally, Alice should use a separate key for the SHA-256 HMAC authentication, which should not be derived from the AES key.

When verified if HMAC matches the received HMAC, Bob can be confident that the message is authentic and has not been tampered with.

(b) The mistake in this scenario is that Bob is asking a Certificate Authority (CA) to sign his RSA key using the CA's private ECC key. RSA and ECC are different cryptographic algorithms, and their keys are not interchangeable. This mixing of different asymmetric encryption algorithms is incorrect.

Instead, Bob should generate an RSA key pair and have the CA sign his RSA public key using the CA's private RSA key. Alice's browser can then verify the signature using the CA's public RSA key. The fact that the CA's public ECC key is in Alice's browser is irrelevant to the verification process.

(c) The mistake in this scenario is that Alice is using the same key pair for both encryption and signing purposes. It is generally recommended to use separate key pairs for encryption and signing to maintain security.

The correct approach would be, Alice should generate two separate key pairs: one for encryption (ECDH) and one for signing (ECDSA). The recipient's public encryption key should be used to encrypt the email. The Alice can sign a SHA-256 hash of the email using her private signing key. Alice should include the encrypted email and the signature in the SMTP message. Alice should publicize the recipient's public encryption key and her own public signing key.

By using separate key pairs for encryption and signing, Alice ensures that compromising one key does not compromise the security of the other operation. This improves the overall security of the system.

(d) The mistake in this scenario is that Alice and Bob establish a shared secret key using Diffie-Hellman, but then Alice plans to encrypt her bank account number using the shared secret key under AES in counter mode. Without proper authentication an attacker can intercept the communication and impersonates either Alice or Bob.

To mitigate this, after establishing the shared secret key using Diffie-Hellman, Alice and Bob should use a mutual authentication mechanism. This can be achieved by using digital signatures or a separate authentication protocol to ensure that both parties are indeed Alice and Bob. Once the authentication is successful, Alice can encrypt her bank account number using the shared secret key.

Question 2

(a) Superfish can change the contents of an encrypted web page by intercepting the encrypted traffic between the user's browser and the website. It does this by acting as a root certificate authority on the computer, generating fake certificates for the websites the user visits. When the user's browser attempts to establish an HTTPS connection, Superfish presents the fake certificate to the user instead of the website's real certificate. The browser, trusting the fake certificate as a valid one, establishes an encrypted connection with Superfish instead of the actual website. This allows Superfish to decrypt and modify the encrypted traffic between the user and the website.

(b) To generate a valid certificate for a website, the attacker needs to obtain a valid certificate signing request (CSR) from the legitimate website. The attacker can then use the stolen CSR to generate a new certificate that appears legitimate. The attacker would use the same signing key that Superfish used in every laptop computer to sign the certificate, making it appear valid to any computer with Superfish installed. The attacker can then present this fake certificate to users with Superfish, who will trust it due to the presence of Superfish's root certificate authority on the computer.

(c) A careful user can notice that their computer is infected by Superfish by checking the list of installed root certificates in their browser or operating system. Superfish installs its own root certificate authority, which can be found in the list of trusted certificates. By examining the list, the user can look for any unfamiliar or suspicious root certificates, including those related to Superfish. Removing or disabling the Superfish root certificate authority can help protect against the interception and modification of HTTPS traffic.