Ryan Son

CS338

Jeff Ondich

October 6, 2024

Cryptographic Scenarios

1. Alice and Bob can encrypt their message using the symmetric encryption algorithm AES and exchange a secret private key K using the Diffie-Hellman key exchange procedure that allows Alice and Bob to agree on a shared secret. Alice encrypts her original message (M) with the private key (K) by computing AES(K, M) and then Bob decrypts the ciphertext (C) by computing AES_D(K, C).
2. Alice can sign the message using a signature by hashing her message using the cryptographic hash function SHA256. By running the hash function (H) on Alice's message (M) by computing H(M), if anyone were to modify the original message by even one bit, it will result in an entirely different hash value H(MM) where MM is the modified message. Alice and Bob will also need to compute their own public/secret key pairs. This hash is then encrypted using Alice's private key (S_A) which will then create a signature. After Bob receives the signature, he can decrypt the signature by using Alice's public key (P_A) and view the 256-bit hash value. So, if Mal ever edits the original message, Bob can tell by running SHA256 on the received message checking if the SHA256 hash value of the received message is different than the value found within the signature. If the value H(M) is the same, then Bob knows that the original message from Alice was not tampered with.
3. Alice can encrypt the message that she sends to Bob using the symmetric encryption algorithm AES. Then Alice must rely on the help of a trusted third party – a Certificate Authority – to sign her message with a signature and create a certificate that will include her actual public key (P_A)

and will be encrypted by the CA's private key. Bob can then decrypt the signature using the CA's public key and examine the hashed message and know that it was sent by Alice.

4. Question
    a. Alice could claim that the original message was digitally altered by Bob to include the erroneous contract with Alice's signature.
        i. Since the original message was signed, it is possible to examine whether the message that was received (M) by Bob was the original (O), by comparing computed hash value of the original message H(M) and the original hash value H(O). I believe that this situation is plausible and would require the computation and comparison of the above values to conclude who is at fault.
    b. Alice could claim that Bob never confirmed if the message was the original contract because Bob provided Alice's public key as evidence.
        i. To ensure that the actual contract was the correct one, Bob would have needed to decrypt the Sig with his private key (S_B), because Alice would have encrypted the Sig with his public key (P_B). So, Bob's accepting of the contract was negligent. I believe this is plausible,
    c. Alice could claim that someone else (Mal) gave Bob the Mal's public key, intercepted communications between Alice and Bob and altered the original contract C and Signature.
        i. This is very plausible as there is no way for either Bob or Alice to tell if the original contract was altered.
5. Sig_CA would consist of E(S_CA, H(TBS)). CA would encrypt (E) the SHA256 value (H(TBS)) of the original message (TBS – to be signed) with their private key (S_CA). By encrypting the hash

(H(TBS)) with S_CA, it allows the recipient of the signature to decrypt the message with the CA's public key (P_CA) to view (H(TBS)) and check if the received message is the original one.

6. Cert_B sent by Bob to Alice is not enough for Alice to verify that she is talking to Bob. If Bob is to be trusted, he must send his RSA public key (P_B) to Alice. Then Bob's public key must match what should be his private key (S_B). Alice will send a challenge to Bob by telling Bob to encrypt a message of Alice's choice (M) with his private key (S_B) and then send it to back to Alice. If this message is successfully decrypted by Alice using his provided public key and the public key provided by the certificate, then it is really Bob that is sending the message.
7. How can Mal convince Alice that Mal is Bob?
    a. The certificate-based trust system can be subverted by establishing a fake certificate authority that is malicious.
    b. If Mal ever gets a hold of the CA's private key, they can impersonate the CA and forge fake certificates which can be used to mislead both Alice and Bob.