Cryptographic Scenarios

Author: Jeremiah and Ntense

1) Alice wants to send Bob a long message, and she doesn't want Eve to be able to read it. Assume for this scenario that AITM is impossible.

Alice and Bob use Diffie-Hellman to agree on a shared secret from which they derive an AES key K. They may need to break the message into pieces to ensure they can encrypt the whole message. Once the key and message have been prepared the two users should be able to encrypt and decrypt the message securely using their shared key. This plan works because the eavesdropper (Eve) can’t decipher the secret key because of the limited information being transmitted between Bob and Alice when establishing the key. Furthermore, AITM has been ruled out of the scenario so we don’t have to worry about anybody impersonating a user (Mal).

2) Alice wants to send Bob a long message. She doesn't want Mal to be able to modify the message without Bob detecting the change.

Alice and Bob would have to communicate using signatures to ensure the authenticity of the message. Alice would send Bob the message with the unencrypted message concatenated with the signature (M’ | E (S_A, H(M)). After Bob recieves the message he would use Alice’s public key P_A to decrypt the hashed message, H(M), and then proceed to hash the concatenated message using SHA-256 H(M’). Once these steps have been completed Bob can compare the H(M’) with H(M) and if they are the same value you know that the message hasen’t been modified.

3) Alice wants to send Bob a long message (in this case, it's a signed contract between AliceCom and BobCom), she doesn't want Eve to be able to read it, and she wants Bob to have confidence that it was Alice who sent the message. Assume for this scenario that AITM is impossible.

Considering that AITM is impossible, Alice could first sign the the message using her private key, creating a digital signature that can be verified by using Alice’s public key. Then, Alice could use Bob’s public key to encrypt the signed message, ensuring only Bob could decrypt and view the message using his private key.

E(P_B, E(S_A, M)).

4) Consider a scenario where Alice and Bob have been in contract negotiations and sharing documents electronically along the way. Suppose Bob sues Alice for breach of contract and presents as evidence the digitally signed contract (C || Sig) and Alice's public key P_A. Here, C contains some indication that Alice has agreed to the contract—e.g., if C is a PDF file containing an image of Alice's handwritten signature. Sig, on the other hand is a digital signature, as described at 9:23 or so of the Cryptographic Hash Functions video.

Suppose Alice says in court "C is not the contract I sent to Bob". (This is known as repudiation in cryptographic vocabulary.) Alice will now need to explain to the court what she believes happened that enabled Bob to end up with an erroneous contract. List at least three things Alice could claim happened. For each of Alice's claims, state briefly how plausible you would find the claim if you were the judge. (Assume that you, the judge, studied cryptography in college.)

- The contract, C, was modified by a third party somewhere between the transmission between Bob and Alice. This can be confirmed by decrypting the signature, revealing the hashed contract, and hashing the contract C concatenated with sig. Afterward, the judge would simply need to compare but hashed contracts to either support or refute this claim, making this a plausible statement.

- Bob could have been a victim of a replay attack. In this type of attack, an attacker intercepts and records previously encrypted messages between Bob and Alice, even though they cannot decrypt them. To cause confusion or disruption, the attacker resends one of these old messages. This could explain why Bob ended up with the incorrect contract (C). Alice could prove this case by providing the history of their contract negotiations. If the incorrect contract matches a previously sent version, it supports the claim of a replay attack, making this a plausible case.

- Alice could claim that Bob perhaps modified the contract after receiving the message, this could be proven by showing the judge the negotiation history between Bob and Alice, however, this could be slightly harder to prove because Bob can claim some third-party modified the text. This would make the claim less plausible.

5) For this scenario, suppose the assumption that everybody has everybody else's correct public keys is no longer true. Instead, suppose we now have a certificate authority CA, and that everybody has the correct P_CA (i.e. the certificate authority's key). Suppose further that Bob sent his public key P_B to CA, and that CA then delivered to Bob this certificate:

Cert_B = "bob.com" || P_B || Sig_CA
In terms of P_CA, S_CA, H, E, etc., of what would Sig_CA consist of? That is, show the formula CA would use to compute Sig_CA.
Sig_CA = E(S_CA, H("bob.com" || P_B)): The digital signature of the Certificate Authority.

You can authenticate this signature by using the CA's public key.
E(P_CA, E(S_CA, H("bob.com" || P_B))) = H("bob.com" || P_B).

6) Bob now has the certificate Cert_B from the previous question. During a communication, Bob sends Alice Cert_B. Is that enough for Alice to believe she's talking to Bob? (Hint: no.) What could Alice and Bob do to convince Alice that Bob has the S_B that goes with the P_B in Cert_B?
Bob could send Alice an encrypted message using his secret key S_B. Then Alice could confirm Bob's secret key by attempting to decrypt the message with the public key provided in the certificate P_B. If Alice can decipher the message it confirms that Bob has the secret key S_B.

7) Finally, list at least two ways the certificate-based trust system could be subverted from the previous two questions, allowing Mal to convince Alice that Mal is Bob.

- If Mal accessed the CA's private key, he could forge certificates to impersonate others, sending Alice a fake Cert_B with Bob's identity.
- If the CA team went rogue, they could forge a fraudulent certificate for Mal, allowing them to impersonate Bob and intercept or alter Alice's messages.