Cryptographic scenarios HW

Author: Prompt Eua-anant

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.

    a. Answer: Alice/Bob uses Diffie-Helman, with large g, p, and random private keys, to agree on a secret message S, which gets converted to the AES key K. Since the message is long, Alice needs to break M into n-bit chunks so that it fits in the domain of the AES algorithm. For each chunk M_i, Alice can encrypt the message by XORing it with either the previous ciphertext chunk C_{i-1}, or if this is the first time, XOR it with a randommized initialization vector (IV). Then, perform AES(K,M_i) to get ciphertext C_i. Do this for all chunks, and send the IV and all ciphertext chunks to Bob. Bob can decrypt each ciphertext chunk by AES_D(K,C) and perform the appropriate XOR operation.

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.

    a. Answer: Alice should send Bob (M and Sig_A), where Sig_A = E(S_A, H(M)). Once Bob receives M, he can compute H(M) and see if it matches E(P_A , Sig_A). Mal wouldn't be able to modify M and recompute the right Sig_A because they would have to know Alice's S_A.

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.

    a. Answer: Split Alice's message M into chunks M_1, M_2, …, M_n that fit in the domain of E. Then, encrypt each chunk using E(S_A, M_i), and encrypt the result using E(P_B, C_i) to get a ciphertext chunk C_i. Once Bob receives all the ciphertext chunks, he can perform the following operation E(P_A, E(S_B, C_i)). If the result makes sense, then it's from Alice.

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.)

a. Answer:
    i. Bob and I didn't use certificates in our communication. I used public and unprotected wifi to send my documents. Mal must have intercepted my message, modified its contents, and forwarded it to Bob.
        1. Judge: Mal would have to know Alice's private key to compute the right Sig. This is implausible.
    ii. When I finished writing my document C, I went to the bathroom for 5 mins while leaving my laptop open. My colleague must have altered the document and I didn't check before I sent it to Bob.
        1. Judge: plausible but can't guarantee anything yet, need more evidence; perhaps security cameras?
    iii. I left my laptop open, and Bob must have gained access to my private key. After I sent my document to Bob, Bob altered the document, computed its hash value, and encrypted the hash value with my private key to get Sig.
        1. Judge: Bob would have to know Alice's password to read her private key file. Need more evidence.

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? That is, show the formula CA would use to compute Sig_CA.

   a. Answer: Sig_CA = E(S_CA, 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?

a. Answer: It's not enough because it only shows that P_B is bob.com's legit public key, and not that the sender is the legit bob.com. To convince Alice that she's talking to Bob, both of them need to agree on the following scheme. Bob encrypts some message X with S_B and sends it to Alice. Alice decrypts Bob's message using P_B and if the result matches X, then Alice is talking to Bob.

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

    a. Answer:
        i. The CA company was compromised from the inside. Perhaps one of its employers, Mal, modifies Bob's certificate to the following: "Bob.com" || P_Mal || Sig_CA, where Sig_CA is E(S_CA, H("Bob.com" || P_Mal). This means Mal can now send this certificate to Alice to trick her that she's talking to Bob.
        ii. When Bob sends his public key to CA, Mal is able to intercept the message and replace P_B with P_Mal. The CA thought P_Mal is Bob's public key, and issued the certificate "Bob.com" || P_Mal || Sig_CA.