David Toledo

CS 338

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.

    C = AES (K, M)

    C gets sent to Bob

    M = AES_D(K, C)

    This archives the prompt, as by using Diffie-Hellman, we know that Eve cannot compute the correct key efficiently enough to eveasedrop on the conversation.

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 will use a public/secret key pair to exchange information.

    Alice:

    H(M) → E (S_A, H(M)) = Sig

    Send M-Sig

    Bob:

    Separate M and Sig.

    E (P_A, Sig) = H(M)

    If what results from E (P_A, Sig) is the same as the message after being hashed by SHA-256, then Mal has not changed the message at all.

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.

   Alice and Bob will use a public/secret key pair AND Diffie-Hellman to exchange information.

   Alice and Bob use Diffie-Hellman to agree on a shared secret from which they derive an AES key K.

   Alice:

   H(M)

   E (S_A, H(M)) = Sig

   AES(K, M-Sig) = C

   Alice sends C to Bob

   Bob:

   AES_D (K, C)

   Separate M from Sig.

   E (P_A, Sig)

   If this equals H(M), then M has the signature from Alice, while also having the confidentiality factor of Diffie-Hellman.

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.

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.)

Mal intercepted Bob's connection and pretended to be Alice

This could be likely, as if this was all online then Bob could have never been talking to Alice in the first place, and was simply talking to Mal from the beginning. This could be checked by using Alice's public key, instead a potential fake public key from Mal.

Mal replaced the file that Bob was sent

This could have happened if Mal had simply changed the C document in the final communication between Alice and Bob. However, this can be detected by comparing the hashed message in the Signature, and the hashed version given by Mal, as these will produce vastly different hashes with any bit of change.

Bob changed the contract

Similarly, if Bob had changed the contract, then this would be easily detectable, as the original message would be hashed inside of the signature, therefore all that needs to be done is have the message Bob claims is the contract Alice agreed too, and this results in the same hashed message within the signature then this is in fact the same contract.

5. 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.

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`?

   Alice can send a message to Bob which Bob can sign. This signature with this private key would be able to be undone with Bob's public key that Alice has. If the message Alice sends corresponds to what is shown after we undo Bob's signature, then we know that we are 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.

   If Mal could infiltrate the CA and create her own CA certificates, then Mal could convince Alice that she is speaking with Bob while in fact what she has sent is not Bob's certificate.

   Mal could intercept the certificate being sent over to Alice from the CA, and send her own fake certificate which would contain her own public key instead of Bob's.