McKenna Wirth

Consulted with Antonia Ritter

CS338 Spring 2022

Cryptographic Scenarios

Simple Communication Scenarios

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 PITM is impossible.**

Alice and Bob want to send messages to each other, but want to do so in a way that prevents Eve from reading those messages. As these messages are long, they must use symmetric encryption. Alice and Bob should use the Diffie-Hellman key exchange to agree on a shared secret key K over a public, open channel. Once Alice and Bob have K, they can send any message M by using the symmetric encryption algorithm AES and the block cipher mode CBC. Alice would send the ciphertext C =AES(K, M) to Bob and Bob would then decrypt the message M = AES_D(K, C).

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.**

To prevent Mal from modifying messages sent from Alice to Bob, Alice could use the cryptographic hash function SHA-256 to create a digest of the message, which would then be appended to the full text message. H(M) would then be encrypted using S_A and, as the message is long enough that using public key encryption is inefficient, M could be encrypted using AES with a shared secret key K agreed-upon by Alice and Bob using Diffie-Hellman. Alice would send this ciphertext C = AES(K, M||E(S_A, H(M))) to Bob.

Bob would decrypt the message using AES_D(K, C) and decrypt the signature at the end using P_A. Bob can verify that the message was not manipulated in any way by hashing the decrypted message, without the decrypted H(M), also using SHA-256 and comparing that value to the value that Alice appended onto the message before encryption.

As Mal does not have S_A, they cannot re-encrypt a new hash function that corresponds to their changes to M. Therefore, while Mal can add or remove sections of M and, if Mal has K, read M, these changes would be detected when Bob compares the hashes (or if Bob notices sections of M are now gibberish or obviously missing).

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 PITM is impossible.**

Alice should encrypt a hash of the message M with S_A then append this encrypted signature onto M, the entirety of which could be encrypted using AES and a shared secret key K found through Diffie-Hellman. By encrypting H(M) with S_A, Alice also proves that she is the one who sent the message, as she is the only one with S_A. Because the message is long, it is not efficient to use public key cryptography on the entire contract, and the use of Diffie-Hellman to agree on K means that Eve cannot read the encrypted message.

Upon receiving the ciphertext, Bob can decrypt using AES_D(K, C), then further decrypt the signature using P_A and compare it to the hash digest created using the input of the decrypted AES_D(K, C) without the signature. As Alice is the only one with S_A, Bob can be confident that Alice is the one who sent the message and, by virtue of the hash comparison, that the message has not been modified.

Questions About Breaking Security

4. **Consider scenario #3 above. 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. 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) C was altered after Alice sent it, by Mal or by corruption: this claim would be very easy to prove or disprove, as the signature includes a hash digest of the plaintext message. Decrypt and hash C, then decrypt the signature and compare the hash digests. Any differences mean that the message was altered in some way, but if they are the same, the contract was not altered after Alice sent it to Bob.
        i) This could mean that Mal added something to the contract or removed something from the contract. Either of these differences would be tested by comparing the hashes, as described above.
    b) The secret key used to create the signature does not belong to Alice: this is also easy to prove or disprove, as P_A must be able to decrypt S_A. If S_A does not belong to Alice and P_A does, then P_A would not be able to decrypt the signature.
    c) The public key provided to the court does not actually belong to Alice: assuming that Alice is the only one with S_A, this could be proved or disproved by having Alice encrypt a random number R then decrypting it using the value of P_A provided to the court. If the numbers are not equal, P_A is not the correct counterpart to S_A. That would therefore mean that the contract, which was decrypted using P_A as provided to the court, was constructed using a different

secret key that did not belong to Alice (similar to option b above). Given the assumptions for these scenarios, this would be quickly dismissed as an argument and I would render a verdict of guilty.

d) The contract was replaced with another contract that has the same hash: this is very unlikely, as hash functions are designed to avoid this outcome. However, it is always possible that Alice used a flawed implementation.

e) Alice's secret key could have been compromised: this is possible, but knowing little about the legal field as it relates to this sort of lawsuit, I would likely consider that due to Alice's negligence. Furthermore, Alice should have taken steps to amend this breach in security as soon as she noticed the secret key was no longer secret. (Although this reality violates the assumptions for the assignment, it is still an argument that Alice could make in court and an important real-world consideration.)

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

Sig_CA = E(S_CA, H("bob.com" || P_B))

Sig_CA can be decrypted using E(P_CA, Sig_CA) to yield H("bob.com" || P_B), where "bob.com" || P_B is the to-be-signed (TBS) section of the certificate.

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?**

Anyone can obtain Cert_B, as it is public. Alice could encrypt a random integer R with P_B from Cert_B and send it to Bob, asking for him to decrypt it using S_B and send it back to her, likely encrypted with P_A. To avoid a PITM attack, this could also be done after establishing a shared secret key K using Diffie-Hellman and sending back the decrypted R as part of an encrypted message E(S_B, H(K||R)).

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

The certificate authority could be compromised by Mal, Mal could create their own certificate authority and wait until it was widely trusted then issue their own Cert_B, or Mal could trick the certificate authority. All of these situations could result in Mal possessing a certificate claiming Bob's identity.

Mal could also send Cert_B to Alice, who wouldn't know that she is not communicating with Bob unless she attempted to test Mal the second method of encryption for R [sending C = E(S_B, H(K||R)) instead of just R decrypted using S_B] described in scenario 6. Simply asking Mal to reply with R would allow for a successful PITM attack, as Alice could then start a Diffie-Hellman key exchange with Mal instead of Bob.