CRYPTOGRAPHIC SCENARIOS

Vicente Riquelme and Seth Romanenko
04/25/2022

1. Assuming PITM is impossible, Alice and Bob can use a Diffie-Heleman to exchange a key K. Then, they can use this key K to exchange messages through the AES encryption system. Alice's message M is encrypted through AES(K,M) = C, Bob receives C and uses AES_D(K,C) = M and is able to read Alice's message. Eve is unable to decipher this encryption since they don't have K and brute force takes much too long.

2. Assuming that integrity is all that is needed, In order for Bob to be sure that Alice's message was not tampered with, Alice can send a hash digest of their message as well. Alice computes Hash_A = H(M) and sends M || Hash_A.

To confirm the integrity of the message, Bob can hash the message M that they received, such that Hash_B = H(M). If Hash_A != Hash_B, Bob knows that the message was tampered with. If Hash_A == Hash_B, then the message was not tampered with.

3. In this case, Alice and Bob can use a Diffie-Heleman to exchange a key K. Then, they can use this key K to exchange messages through the AES encryption system.

Alice's message M is encrypted through AES(K,M) = C, Bob receives C and uses AES_D(K,C) = M and is able to read Alice's message without Eve eavesdropping. Alice also includes a Hash_A = H(M), which she encrypts with her private key as HAE = E(S_A,Hash_A) and sends it to Bob.

Bob can then decrypt what he receives through Hash_A = (E(P_A, HAE). He also hashes what he receives in the message, Hash_B = H(M). If Hash_A == Hash_B, he knows the message hasn't been tampered with and also that Alice is the person with that secret key, since it was decoded with the other public key.

4. Three things that could have happened for Alice to have not sent that contract. Assuming that someone else does not have Alice's private key:

   1. Some outside agent, MAL, pretended to be Bob when talking to Alice and pretended to be Alice when talking to Bob. Thus, everything was sent through Mal, which could have caused the contents to be forged in a way that Alice and Bob cannot detect. This is likely what happened if Bob and Alice were not able to confirm each other's identities. However, Bob is only able to decrypt a hash sent by Alice if the sender did in fact have the secret key S_A, and vice versa. Therefore, a successful decryption using P_A guarantees that the sender was in fact in possession of the correct secret key, S_A.
   2. Someone brute forced her key. This is a practically impossible scenario as there are total of $1.1\ x\ 10^{77}$ possible keys that can be used for AES 256 encryption. In order to correctly derive the correct key by brute force, an inordinate amount of computational power

would be required, making this method impossible with our current technological capabilities.

3. It is possible that an altered document had the same hash as the original one. However, this is unlikely since Hashing Algorithms are designed to prevent these kind of attacks. Also without knowledge of one’s private key, it is nearly impossible to forge.

5. Sig_CA = E(S_CA, H(E(P_CA, DATA)

6. Having determined P_B from Cert_B, Alice could ask Bob to send a message, L, in order to verify his identity. This message would be random to prevent another phisher from already having it. Alice would also ask Bob to encode L with his private key, S_B. Bob sends T = E(S_B, L) to Alice who, in turn, is able to verify that L = E(P_B, T). Thus, when Alice checks the message with P_B and it is valid, Alice knows that Bob is indeed in possession of S_B and can be trusted.

7.

1. Mal could convince the public authority that they are Bob by using a public key.

2. If the certificate authority is unknown or untrusted, they could potentially be working either against the interests of Alice and Bob or directly with Mal. Since the CA is the party responsible for generating and providing both the public and private keys for Alice and Bob, they can exploit this trust and convince Alice that they are actually Bob. This particular vulnerability makes it crucial that the CA is verified and reputable.