Scenarios

Zitian Yue

April 26, 2022

1. Alice and Bob use Diffie-Hellman key exchange to agree on a shared secret key K. Then Alice breaks her message into several blocks of certain size and employs AES encryption on every block. She eventually sends those encrypted blocks to Bob.

Without worrying about the PITM attack, Diffie-Hellman key exchange is a secure method for the negotiation between Alice and Bob. There is currently no efficient way for the Eve to solve this discrete algorithm. Thus, Eve does not know value of K and can not read the encrypted message even though algorithm of AES is known.

2. Alice and Bob use hash function to protect the integrity of the message.

Alice gets a hash of her message by: $D = H(M)$ and concatenates her message M with D to send to Bob. Bob then repeats the process of hash $H(M)$ based on M received from Alice. He can compare whether D received from Alice is equivalent to his own calculation $H(M)$. Since the hash function will generate an entirely different result even though slight change is made, Bob always detects change made by Mal as the changed message will lead to a distinctive value of $H(M)$ which does not equal to D.

3. Alice and Bob use the public/secret key pairs to provide authenticity of Alice's identity. They use the Diffie-Hellman key exchange to agree on a shared secret key K.

Alice employs Diffie-Hellman key exchange to negotiate with Bob about a shared key K. She then does AES encryption $AES(K, M)$ and does another encryption $E(S_A, AES(K, M))$ based on her own secret key. In this way, Bob can confirm Alice's identity since he can use Alice's public key to decipher the message received. Eve is not able to read the message even though Alice's public key is known. This is because there is another layer of encryption based on shared key K between Alice and Bob.

4. Few things that could happened are:

- There exists a MAL who intercepts and changes the contract sent from Alice to Bob. If I were the judge, I find this explanation reasonable since Alice and Bob did not employ any technique in preventing the PITM attack.
- Alice is not the "Alice" who sent the contract to Bob. This means that the public key provided by Bob is actually not Alice's public key. This explanation is not considerably solid but plausible. If Bob negotiates with fake "Alice" for encryption, the contract would be based on unreliable sources.
- The contract is altered by Eve. This explanation is not plausible since Eve does not have Alice's secret key. The authenticity of Alice's identity is confirmed by Bob with employment of public/secret key pairs.

5. Bob will sends his public key P_B to the certificate authority first by $E(P_{CA}, \text{"}bob.com\text{"}||P_B)$. CA will use its secret key S_{CA} to retrieve Bob's message by $E(S_{CA}, E(P_{CA}, \text{"}bob.com\text{"}||P_B)) = \text{"}bob.com\text{"}||P_B$. After the CA miraculously identifies Bob's identity, it then derives $Sig\_CA = E(S_{CA}, H(P_B))$. Sig_CA will be combined with $\text{"}bob.com\text{"}||P_B$ to form the certificate.

6. Alice should not believe the authenticity of "Bob" since certificate can be fabricated as well. To convince her, Alice should contrive some testing message M and encrypt it with Bob's public key P_B

in $Cert\_B$. Alice then sends the encrypted message to Bob and request for a reply of decryption. Bob should then use his secret key S_B and try retrieve the testing message M. Bob will send that message back to Alice so that Alice can compare to make sure she's talking to Bob.

7. Few ways how this certificate-based trust system could be subverted are:

- The certificate authority trusted by Alice is actually manipulated by Mal. This means that Mal can send a fake certificate containing public key that can be resolved to Alice and claim to be Bob. Alice is likely to be convinced since her attempt of testing can be satisfied.
- Mal is such a good thief who manages to steal the secret key owned by CA S_{CA} from the server physically. Since the public key P_{CA} is known online. Mal can now convince Alice that Mal is Bob since any attempts of testing made by Alice can be satisfied.