Scenarios

By: Sydney Nguyen

SIMPLE COMMUNICATION SCENARIOS

1. To stop eve from being able to read the message interaction between Alice and Bob we must use symmetric encryption, in other words, the Diffie-Hellman exchange. To begin the exchange Alice and Bob must both decide on the secret key. K, which Eve will not be able to know because she is not in the middle of the exchange but rather just eavesdropping. Once the secret key is agreed upon Alice can encrypt their message, M, by sending the cyphered text C = AES(K, M) then bob will be able to decrypt the message by AES(K, C). Eve will not know K so she will be unable to decrypt the message.

Defined Variables:

K = secret key
C = encrypted message
M = Long message

2.

It is important to note that we want to avoid PITM interference more specifically we want to avoid Mal from being able to modify the message. To notice any small modification to the message it is important to use the cryptographic hash function SHA-256. In other words, Alice needs to hash her message M, $S = E(S_A, H(M))$. Alice then sends M||S. When Bob receives the data, possibly tampered with by Mal, and then uses Alice's public key, P_A, to $E(P_A, M) = E(P_A, E(S_A, H(M)))$ and checks that the encrypted message equates what Alice sent over. In other words, Bob applies SHA-256 to the message received. If the messages are equal then Mal has not been able to edit the message and if the message is not then Mal has been able to edit the message. It is important to bring to light that this works because with SHA-256 any slight change to the original message will produce a strikingly different C. We must use SHA-256 and not public-key encryption because we want to encrypt a long message and the public key is exclusively for short messages.

Defined Variables:

S_A = Alice's secret key
P_A = Alice's public key
S = signature
C = encrypted message
M = Long message
H = hash function

3.

It again is important to note that it is impossible for PITM to come between Alice and Bob. To start Alice and Bob should use the Diffie-Hellman encryption and decide on a shared secret key. Alice encrypts message M with K, therefore, computing AES(K, M) = C. After Alice encrypts the message to C she then will hash C to get her signature. S = E(S_A, H(M)). Then Alice will send C|| S to Bob. Bob will then hash the message and decrypt Alice's signature by using their Public Key. Bob will attempt to E(P_A, S) then check that the information he decrypted matches the information Alice sent.

Defined Variables:

S_A = Alice's secret key
P_A = Alice's public key
S = signature
C = encrypted message
K = secret key
M = Long message
H = hash function

QUESTIONS ABOUT BREAKING SECURITY

4.

a. Claim 1: Alice’s private key was compromised or sent without Alice’s permission.

   i. This is not plausible because if Alice’s private key was compromised Bob would not have been able to decrypt the message. For Alice’s private key to be sent without her permission is slightly plausible however someone, maybe Mal must have been able to breach Alice’s computer.

b. Claim 2: Mal was able to modify the message without Alice or Bob’s knowledge.

   i. This is very unlikely or not plausible because Mal would both have to find the K, secretly shared the key, and change the message. However, it is important to note that this would only be able to occur if Bob is very negligent and does not check the signature.

c. Claim 3: A false contract, either Bob did not decrypt the message correctly, or there is another contract with the same hash.

   i. It is somewhat plausible that Bob did not decrypt the message as human error is a thing, but he really would not understand how to decrypt to have the wrong contract. It is not very plausible that the same hash would be produced is $1.47*10^{-29}$.

5.

$Sig_{CA}= E(S_{CA}, H(\text{"bob.com"}|| P_B))$

6.

No! Alice and Bob can start with using the Diffie-Hellman encryption to being the process to prove that S_B that goes with the P_B in Cert_B. After the key is agreed upon Alice can send bob a message C which bob can reply to using E(S_B, H(K||C)). Alice will then be able to confirm Bob's public key using her own equation with hash, message, and r. If all goes well we can confirm that the person she is communicating with is in fact Bob or using Bob's key.

7.

a. Mal acquires Bob's secret key by brute forcing or hacking his computer
b. Mal could request a certificate for bob.com and then she can send alice the newly gained certificate.
c. Mal could literally just PITM and intercept all the keys and information being shared.

Cite

https://www.avira.com/en/blog/md5-the-broken-algorithm