Matthew Krieger & Chelsea Edwards

CS 492

Homework 8

1)

{[Alice,R1,ga mod p]Alice}Bob ----->

<----- {[R1,R2,gb mod p, h(gab mod p)]Bob}Alice

Session key h(R1,R2,gabmod p)) ---->

Alice and Bob forget R1, R2, a and b

2) Trudy can initiate a connection with Bob saying “I’m Alice”, R together with random value R. Bob in response will send E(R, KAB) to Trudy. Now, since Trudy don’t know KAB, she can’t compute E(R+1, KAB), but she can initiate a new connection with Bob by saying, “I’m Alice”, R+1 together with R+1 value. Trudy already knew what value of R she sent before, so she can just sent R+1 next time. Now, Bob in response will send E(R+1, KAB). That’s what Trudy needed for previous connection, so using first connection she can send E(R+1, KAB) to Bob. That’s it. The mutual authentication has been approved by this protocol to Trudy claiming she is Alice. Bob will have no idea that he is talking to Trudy instead of Alice. Second, Trudy can perform replay attack.

3)

A) Yes, she tries in line three with {S}BOBbecause only Bob should have the private key to decrypt S.

B) No, he takes in the third line where he uses his private key to get S and receive theE(CLNT, K) with established session key K. The session key is only for messageread/write protection. In the 4thline, Bob then sends Alice, new data with current sessionkey, but never sends her some sort of challenge to authenticate her.

4)

a) Without the nonces, there is no guarantee that the message is “fresh”-- i.e. preventing replay of Alice’s message. This would lead to Alice’s message susceptible to attack by Trudy, who can replay and obtain K if they were listening in.

b) An HMAC by itself doesn’t provide integrity, but it can add to the integrity of the message. It provides a digital signature that prevents an attacker like Trudy from altering the data within the message and verifies the data further as being signed by the sender.

c) Without the encryption, the communication for the channel is actually still secure. The real prevention with Trudy attacking is the digital signature attached to {S} by Bob, which means that Trudy cannot alter or replace that very important part of the hash needed for the key. The encryption that is originally there is an unnecessary step, and adds nothing more to the protective layer of the channel.

5)

A) She can’t remain anonymous because her username and password are first used to login to the system. Furthermore, in Kerberos, a key (KA) is derived from Alice’s password. This is the key that Alice and the KDC share. Alice’s computer uses the key to get the TGT from the KDC. In a nutshell, she is not anonymous because her public key is used to obtain her TGT from the KDC.

1. She remains anonymous because the TGT is encrypted with the key KKDC . Therfore, the KDC does not need to know who is making the request. Aside from the initial login, the entire security process is transparent to Alice.
2. She remains anonymous because Bob decrypts the “ticket to Bob” with his key (KB) to get KAB, which is used to verify the timestamp and to protect the confidentiality and integrity of their conversation. Aside from the initial login, the entire security process is transparent to Alice.