Assignment 10

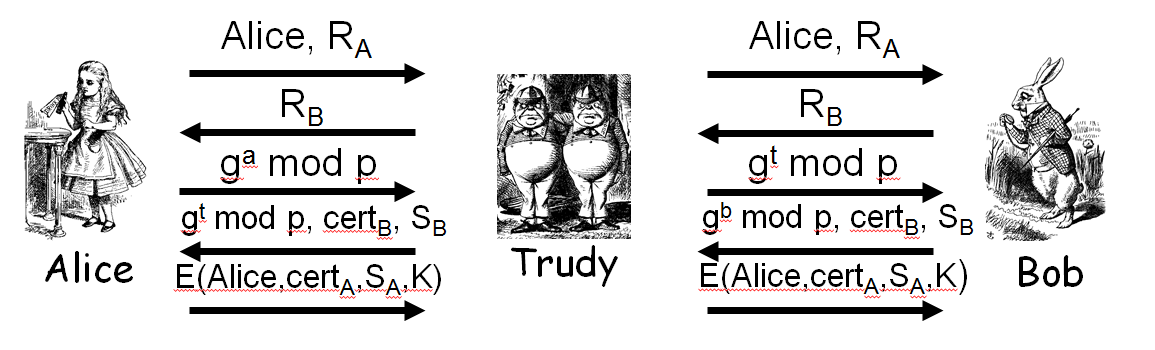
1. **Consider the SSH protocol in Figure 10.1.**
   1. Explain precisely how and where Alice is authenticated. What prevents a replay attack?

In Figure 10.1, Alice is authenticated at the last message where she sends E(Alice, certificateA, SA, K), SA is signed by Alice using her private key therefore it authenticates Alice. This protocol prevents a replay attack because SA is signed by Alice and the content signed inside SA contains the RB which is a random challenge sent by Bob and it will be different next time.

* 1. If Trudy is a passive attacker (i.e., she can only observe messages), she cannot determine the key K. Why?

By being a passive attacker, Trudy cannot determine key K because this protocols uses Diffie Hellman and Trudy can only see ga mod p and gb mod p, but she cannot determine gab mod p.

* 1. Show that if Trudy is an active attacker (i.e., she can actively send messages) and she can impersonate Bob, then she can determine the key K that Alice uses in the last message. Explain why this does not break the protocol.

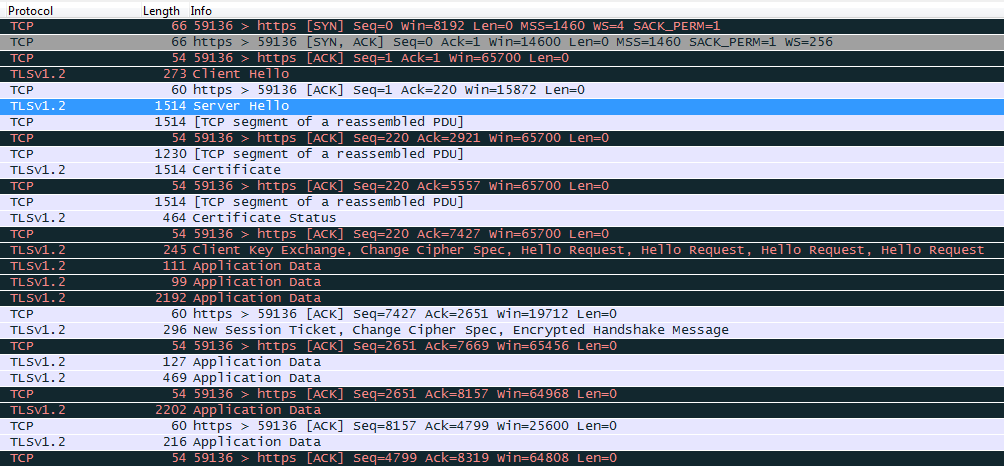


Trudy can determine the key K that Alice uses on the last message by performing a Man in the middle attack, Trudy can simply replace ga mod p with gt mod p on the 3rd message, and on the 4th message, alice replaces gb mod p with gt mod p and then Trudy will be able to determine key K which is gat mod p, but the protocol will fail because integrity check will show that something went wrong on the protocol.

* 1. What is the purpose of the encrypting the final message with the key K?

The purpose of encrypting the final message with key K is to prevent from Trudy from being able to see the contents of the message which includes a hash of all public information together with the only private information which is the session key K = gab mod p.

1. **Use Wireshark [328] to capture SSL authentication packets.**
   1. Identify the packets that correspond to the messages shown in Figure 10.4.



The packet saying “Server Hello” is equivalent to the “Can we talk? Cipher list, RA” message in figure 10.4 “certificate” packet is the 2nd massage in figure 10.4 which corresponds to “certificate, cipher, Rb”

* 1. What do the other SSL packets contain?

The other ssl packets contain encrypted data that we are sending and receiving such as active http connections, etc.

1. **SSL and IPSec are both designed to provide security over the network.**
   1. what are the significant similarities between the two protocols?

The significant similarities of IPsec and SSL is that they both provide Encryption, Integrity check and authentication.

* 1. what are the significant differences between the two protocols?

SSL operates in socket layer while IPSec operates in network layer. IPSec is built-in to the OS therefore applications do not need to deal with IPSec security since it works at network layer it will automatically protect data that goes through it, in the other hand SSL has to be implemented by the application because it is a socket layer.

1. **Consider the Kerberos interaction discussed in Section 10.5.2.**
   1. Why is the ticket to Bob encrypted with KB?

Ticket to bob is encrypted with KB so that Trudy cannot see KAB which is the session key.

* 1. Why is "Alice" included in the (encrypted) ticket to Bob?

“Alice” is included in ticket to bob because Bob only uses KB to decrypt the all the tickets and after decrypting the ticket, Bob can see who he is talking to.

* 1. In the REPLY message, why is the ticket to Bob encrypted with the key SA?

In the reply message ticket to bob is encrypted with SA because ticket to bob is not the only thing inside the REPLY message, the session key KAB is also on the REPLY message therefore it needs to be encrypted to prevent Trudy from knowing KAB

* 1. Why is the ticket to Bob sent to Alice (who must then forward it to Bob) instead of being sent directly to Bob?

If we wend the ticket to bob, bob would need to remember that ticket until Alice decides to stop communicating with Bob, but in the other hand, if Alice has the ticket to Bob, then Bob can be stateless and therefore it does not have to remember any session key.

1. **Consider the Kerberos interaction discussed in Section 10.5.2.**
   1. What is a TGT and what is its purpose?

TGT is a ticket granting ticket that is given by Kerberos, by using the TGT that Kerberos initially gave it to Alice, it proves to Kerberos that Alice has already logged in, so Kerberos will issue tickets to whoever Alice request. TGT is required so that Kerberos can be stateless, so that it does not have to remember who logged in and who didn’t, with the TGT Kerberos can know who did and who didn’t.

* 1. Why is the TGT sent to Alice instead of being stored on the KDC?

TGT is sent to Alice instead of being stored in the KDC because Kerberos need to stay stateless, and it cannot do so by storing TGTs in KDC, therefore TGT is sent to Alice and every time Alice needs a ticket from the KDC she will need to send over the TGT.

* 1. Why is the TGT encrypted with KKDC?

TGT is encrypted with KKDC so that KDC can trust the information inside the TGT, which proves Alice’s identity and protects Alice’s SA key so that KDC can use it to decrypt the authenticator with timestamp.

* 1. Why is the TGT encrypted with KA when it is sent from the KDC to Alice's computer?

TGT is encrypted with KA because TGT is like a session key to Kerberos and by encrypting it, it will prevent intruders from getting it, also TGT is sent together with the SA therefore an encryption is also needed to protect the SA from being seen by intruders.

1. **In IKE Phase 1 digital signature main mode, proof A and proof8 are signed by Alice and Bob, respectively. However, in IKE Phase 1, public key encryption main mode, proofA and proofB are neither signed nor encrypted with public keys. Why is it necessary to sign these values in digital signature mode, yet it is not necessary to public key encrypt (or sign) them in public key encryption mode?**

In Digital Signature main mode, It is necessary to sign the values proofA and proofB to proof your own identity, else there will be no way for Bob to know if it is really alice, as well as there is no way for Alice to know if she is really talking to Bob.

In Public Key encryption main mode, it is not necessary to sign proofA and proofB, because RA and RB has been encrypted using the public key of the other person, and they are authenticated by being able to decrypt it with their private key and get RA and RB and use it to compute K and then use it to compute the hash of the SKEYID.

1. **We say that Trudy is a passive attacker if she can only observe the messages sent between Alice and Bob. If Trudy is also able to insert, delete, or modify messages, we say that Trudy is an active attacker. If, in addition to being an active attacker, Trudy is able to establish a legitimate connection with Alice or Bob, then we say that Trudy is an insider. Consider IKE Phase 1 digital signature main mode.**
2. As a passive attacker, can Trudy determine Alice's identity?

No, Trudy cannot determine Alice’s identity because all names are encrypted

1. As a passive attacker, can Trudy determine Bob's identity?

No, Trudy cannot determine Bob’s identity because all names are encrypted

1. As an active attacker, can Trudy determine Alice's identity?

Yes, Trudy can determine Alice’s identity by performing a man in the middle attack by changing the gb mod p into gt mod p. and then when Alice send the 5th message, Trudy will have K to decrypt the message and see that it is “Alice”.

1. As an active attacker, can Trudy determine Bob's identity?

No, Trudy cannot determine Bob’s Identity because even if Trudy performs a man in the middle attack, and changes the diffie hellman part, when bob receives proofA, Bob will find out that it does not matches and therefore terminate the protocol.

1. **Recall that IPSec transport mode was designed for host-to-host communication, while tunnel mode was designed for firewall-to-firewall communication.**
   1. Can transport mode be used for firewall-to-firewall communication? Why or why not?

The answer to this question depends on where the data is being encrypted, if the Encryption/Decryption is done by Alice and Bob with firewalls in between then Transport mode will not work because the firewalls cannot decrypt the data and look at the TCP header and the application header.

In the other hand, if the encryption is done by the Firewall, then it will work because the firewall will be able to decrypt and check for the TCP and application headers.

* 1. Can tunnel mode be used for host-to-host communication? Why or why not?

In a host to host communication, tunnel mode can be used because there are no firewalls in between and tunnel mode only has more information compared to transport mode, therefore if we use tunnel mode in host to host, we can simply decrypt the data and use it.

1. **Suppose that IPSec is used from host to host as illustrated in Figure 10.16, but Alice and Bob are both behind firewalls. What problems, if any, does IPSec create for the firewalls under the following assumptions.**
   1. ESP with non-NULL encryption is used.

If non-null encryption is used then the firewall will not be able to look into the packet for TCP headers and application headers.

* 1. ESP with NULL encryption is used.

If ESP is used with null encryption, the firewall can know that ESP is being used because of the ESP header, but the header does not specify that it is encrypted with null, therefore the firewall still cannot look into the packet for TCP and application headers.

* 1. AH is used.

If AH is used, it will not create any problems because the firewall will know that AH is used and it knows that nothing is encrypted, therefore it can check for TCP, applications header,etc.

1. **WEP is supposed to protect data sent over a wireless link. As discussed in the text, WEP has many security flaws, one of which involves its use of initialization vectors, or IVs. WEP IVs are 24 bits long. WEP uses a fixed long-term key K. For each packet, WEP sends an IV in the clear along with the encrypted packet, where the packet is encrypted with a stream cipher using the key KIV = (IV, K) , that is, the IV is pre-pended to the long-term key K. Suppose that a particular WEP connection sends packets containing 1500 bytes over an 11 Mbps link.**
   1. If the IVs are chosen at random, what is the expected amount of time until the first IV repeats? What is the expected amount of time until some IV repeats?

If the IV is chosen at random, we only need 2n/2 to find a repeat, therefore it will take:   
1500 \* 8/(11 \* 106) \* 224/2 = 4.47 seconds for the first IV to repeat to get two repeats, it will take 1500 \* 8/(11 \* 106) \* sqrt(2\* 224) = 6.32, therefore for each additional 1.5~ seconds, another IV will be repeated.

* 1. If the IVs are not selected at random but are instead selected in sequence, say, IVi = i, for i = 0, 1, 2, ... ,224- 1, what is the expected amount of time until the first IV repeats? What is the expected amount of time until some IV is repeated?

If IV is selected in a sequence, we would have to go through all the IVs before repeating the sequence, that would take: 1500 \* 8/(11 \* 106) \* 224 = 18302 seconds for the first IV to repeat, and then every message sent after 18302 seconds will have a repeated IV.

* 1. Why is a repeated IV a security concern?

Because IV is used to prevent intruders from deriving the key based on the messages and if the IV is repeated, then it will act as if there is no IV, therefore allowing the intruder to derive the key from the messages.

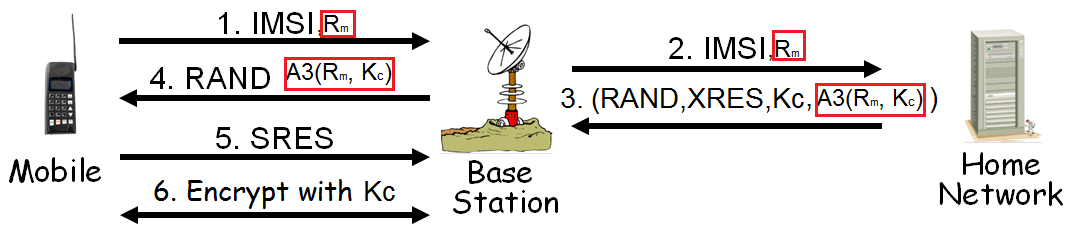
1. **On page 379 it is claimed that if Trudy knows the destination IP address of a WEP-encrypted packet, she can change the IP address to any address of her choosing, and the access point will send the packet to Trudy's selected IP address.**
   1. Suppose that C is the encrypted IP address, P is the plaintext IP address (which is known to Trudy), and X is the IP address where Trudy wants the packet sent. In terms of C, P, and X, what will Trudy insert in place of C?

Since C is encrypted by XOR with a keystream and we have P, we can do C ⊕ P to get the keystream K, with K we can encrypt X by doing X ⊕ K and then use it to replace C.

* 1. What else must Trudy do for this attack to succeed?

Trudy will also need to change the CRC in way that it does not differ from the original CRC, so that the protocol does not detect any errors.

1. **Modify the GSM security protocol, which appears in Figure 10.25, so that it provides mutual authentication.**



Since Ki is only known by the home network and the mobile, we can use Kc which is the hash of Ki and RAND to encrypt the nonce Rm sent by the mobile and then send it back to the mobile so that the mobile can authenticate the home network.

1. **In GSM, each home network has an AuC database containing user keys Ki. Instead, a process known as key diversification could be used. Key diversification works as follows. Let h be a secure cryptographic hash function and let KM be a master key known only to the AuCs. In GSM, each user has a unique ID known as an IMSI. In this key diversification scheme, a user's key Ki would be given by Ki= h(KM, IMSI), and this key would be stored on the mobile. Then given any IMSI, the AuC would compute the key as Ki= h(KM, IMSI).**
   1. What is the primary advantage of key diversification?

The advantage of key diversification is that there is no need to keep a database of Ki keys and it will never expose Ki because it is not stored and it is calculated with hash every time it is needed.

* 1. What is the primary disadvantage of key diversification?

The primary disadvantage of key diversification is that if KM is compromised then all phones/sim cards will have to be replaced because the Ki of every mobile will be compromised, therefore it will require a lot of work to fix if RM is compromised.

* 1. Why do you think the designers of GSM chose not to employ key diversification?

I think designers of GSM did not choose key diversification because of the risk of compromising RM, which would compromise the entire system.