CS 554 Homework #5

Due: Thursday, April 28

Alexander Powell

1. The following protocol shows how Bob chooses whether to require Alice to send a cookie:

   If Bob wants a cookie, then Bob should reply to the message without a cookie with a message like: "please send your message again, but this time returning this "cookie"".

2. It is possible to show a protocol that hides both identifiers from an active attacker. To do this, Alice would send her name as well as her public encryption key certificate and her Diffie-Hellman value encrypted with Bob's public key. Bob would then send an encrypted reply with Alice's public key.

3. (a) The first variant illustrates the scenario where the attacker can learn only the intiator's identity. It is described as follows:
   - First, both parties perform a Diffie-Hellman key exchange.
   - Next, the initiator send their ID and proof of knowledge of the shared key, which has been encrypted with the Diffie-Hellman key.
   - Finally, the target sends their ID and proof of knowledge of the shared key, which has been encrypted with the Diffie-Hellman key.

   By doing this, we have devised a protocol based on pre-shared secret keys that hides the identities and gives PFS for identity holding.

   (b) The second variant describes the scenario in which an active attacker can learn only the target's identity.
   - The first message that is sent is a Diffie-Hellman number.
   - The second message sent contains the Diffie-Hellman number and the target's ID and proof of knowledge of the shared key, encrypted with the Diffie-Hellman key.
   - Finally, in the third message the initiator sends their ID and proof of knowledge of the shared key, encrypted with the Diffie-Hellman key.

   By doing this, we have devised a protocol in which an active attacker can learn only the target's identity.

4. Bob knows that it's really Alice since Alice has proved that she knows the secret key. The key is a function of the nonce and the Diffie-Hellman value which is signed by Alice. However, it's possible that someone could steal an a and the $g^a mod p$. If they were able to do this, then they would be able to impersonate Alice to Bob. It should be noted that the chances of someone being able to steal an a is quite slim. Also, if Alice uses a different a each time she sens a message then she knows she's really talking to Bob. On the other hand, she doesn't know this if she reuses the same a over and over again.

   To modify the protocol to allow both Alice and Bob to reuse their a and b values, and yet have both sides be able to know they are talking to a live partner, Alice should send a nonce as her first message, and let the key be a function of both nonces as well as the value returned from Diffie-Hellman.

5. To ensure that his connection attempt will succeed even if he changes the secret, he should send it as a cryptographic hash. In this way, only the responder needs to know the hash value. In fact, the secret should be changed periodically to prevent "cookie jar" attacks where an attacker accumulates lots of cookies from lots of IP addresses over time and then replays them all at once to overwhelm the responder.

6. No, Bob's IPsec implementation will not notice that the packet is a duplicate. IPsec treats a retransmitted TCP packet as a new IPsec packet. It is the job of the TCP to determine whether a packet is a duplicate.

7. It is possible for the SA to be defined only by the destination address ans the SPI. Because the SA is the receiver that defines the SPI, it can assign different SPIs to ESP or AH. An implementation of a receiver that defined the SA based solely on destination address and SPI will interwork with implementations that allow the same SPI to be assigned to both, and it will distinguish which SA it belongs to based on whether it's ESP or AH.

8. Consider the example where a part of the intranet is connected to the internet with firewall A, and another part of the same intranet is connected to the internet through two firewalls, B and C. It is the case that all addresses in the parts in the intranet described previously equally reached through B and C. Also, we know that SAs come in pairs, so A has two SAs. One SA is pointed to B and the other to C. So, any packets sent from A will either have a key for the $A-B$ SA or the $A-C$ SA. When it comes to the internet routing the packet, it could choose a different firewall than A expected and the delivery will not succeed. Because of this, it is necessary for A to specify which firewall the internet needs to deliver the packet to.

9. The advantage would be that it would be a simpler process because $F1$ could forward the packet to $F2$ without doing a second encryption. However, a disadvantage would be that this transmission would not be as secure, because it was only encrypted once.

10. (a) Relevant fields of the IP header as given to A's IPsec layer
    - source = A
    - destination = B

    (b) Relevant fields of the IP header as transmitted by A
    - source = A
    - destination = B
    - protocal = ESP or AH
    - esp header next header = TCP

    (c) Relevant fields of the IP header as transmitted by $F1$
    - source = $F1$
    - destination = $F2$
    - protocol = ESP
    - esp header next header = IP

    (d) Relevant fields of the IP header as received by B
    - source = A
    - destination = B
    - protocal = ESP or AH
    - esp header next header = TCP

11. If there is an active attacker, the vulnerability lies in the fact that the attacker could trick Alice into using weak cryptography. In this case, the attacker has the ability to impersonate Bob to Alice and reject Alice's strong crypto. At this point, Alice will try again but this time with a weaker proposal.

12. Let's denote the person trying to construct an entire IKE key exchange with a C. To do this, C would choose Diffie-Hellman numbers a and b as well as nonces for each side. Because C has chosen the nonce themself, they are able to establish a "proof of identity" because they can calculate the function of the other side's nonce (since they chose it), as well as the Diffie-Hellman values and the cookies. Additionally, C is able to calculate the session keys because they have access to all variables as well as $g^{ab} mod p$.

13. In the shortened version, the two parties exchange their CP and CPA. Next, one side sends the other the calculation of $g^{ab} mod p$. This method does not allow parallel computation of $g^{ab} mod p$ because unlike the 6-message version, the modular calculation has to be done with both a and b, so the two sides cannot calculate $g^a mod p$ and $g^b mod p$ individually like normal.

14.
    - Photuris hides both the initiator's and the responder's IDs from eavesdroppers. However, for more active attackers, Photuris will only hide one party's ID as the other has to prove their indentity first.
    - With IKE Main mode, both the initiator's and the responder's IDs are hidden from eavesdroppers, but again, one party's ID is exposed to more active attackers since they have to prove their identity at the beginning.
    - With IKE Aggressive mode, neither the initiator's nor the responder's IDs are hidden from eavesdroppers or more active attackers.
    - Finally, with IKE Aggressive and Main mode, both party's IDs are hidden from both eavesdroppers and more active attackers.

15. First, the side with the public signature key would compose the first message and then encrypt it using the other sides encryption key. They would then sign it using their own public signature key. Next, the other side would receive the message, and decrypt it using a function of the public signature key and the public encryption key.

16. Suppose the two individuals attempting to communication are denoted by A and B.

    With only a public signature key, A has no key and know's they're talking to B although B does not know if they're talking to A. First, A sends $g^a mod p$ to B. B then signs with his Diffie-Hellman number and sends back the hashed $g^{ab} mod p$ along with the signed $g^b mod p$ back to A. Finally, A responds with the newly hashed $g^{ab} mod p$

    With only a public encryption key, again A has no key and know's they're talking to B although B does not know if they're talking to A. First A sends $\{g^a mod p\}_B$ to B. B needs their decryption key in order to decipher $g^a mod p$. B then sends back $g^b mod p$ and the hashed $g^{ab} mod p$. Finally, A sends back their own hashed $g^{ab} mod p$.

17. An eavesdropper or active attacker cannot calculate SKEYID because the nonces are encrypted with the public keys of Alice and Bob. More specifically, one of the nonces is encrypted with Bob's public key and the other is encrypted with Alice's public key. Both of these need to be known in order to compute SKEYID.

18. PFS, as implemented in SSL v3, has the client perform an RSA encryption as well as verify the signature using RSA. In both of these cases, the public key is used. The server then decrypts and signs for every authentication. In the decryption step secret keys are used.

    Using the recommended modification, the server doesn't have to perform nearly as many signings. However, using this method makes it necessary for an expiration date to be established and requires clocks to be on the same time.

Finally, using Diffie-Hellman, each side of the exchange has to perform a Diffie-Hellman exponentiation and the server has to sign it's Diffie-Hellman number on each transaction. Note: it is possible for the server to use it's Diffie-Hellman b value more than once.