CSC474 - Information Systems Security: Homework3 Solutions

April 18, 2005

1. (20 points) Harry is given a job as network administrator for a Microscape. His assignment is to setup a firewall for the company. He decides to use a simple packet filtering firewall. Unfortunately Harry is not familiar with firewalls and needs some help setting up his system. The topology of his network is shown below. The Microscape network uses 10.1/16 addresses.

   (a) (5 points) Write a simple rule(s) that allows Microscape employees to browse the Web. Make this rule(s) as restrictive as possible (i.e. it should not let other traffic into/out of Microscape if possible).

Src Addr	Dst Addr	Src Port	Dst Port	Protocol	Action
10.1/16	*	*	HTTP	TCP	allow
*	10.1/16	HTTP	*	TCP	allow

   (b) (5 points) Suppose there were two hosts (A and B) inside the Microscape network. Assuming just the rules you added in a), could an attacker in the Internet still perform a bandwidth denial of service attack that interferes with traffic between host A and B? Why or why not?

   Yes, it can be done by sending SYN packets to A or B, which is allowed by the rules we have added.

   (c) (5 points) Harry installs an HTTP caching proxy in the Microscape network. He wants to ensure that all clients in Microscape use this proxy to browse the Web. How should he modify his rules from a) (you may write out the new rule or explain the changes)?

   Suppose the Proxy is 10.1.1.2:8080, the rules become

Src Addr	Dst Addr	Src Port	Dst Port	Protocol	Action
10.1.1.2	*	*	HTTP	TCP	allow
*	10.1.1.2	HTTP	*	TCP	allow

   (d) (5 points) Assuming the resulting setup from c) and that the web proxy is not one of the links between host A and B, can transfers between A and B be affected by a denial of service attack?

   No. Because the attack can attack the proxy only.

2. Devise a protocol based on a pre-shared secret key that hides identities and gives PFS for identity hiding. Make two variants, one in which an active attacker can learn only the initiator's identity, and one in which an active attacker can learn only the target's identity.

Messages 1 and 2: Diffie-Hellman exchange.

- **variant in which active attacker can learn initiator's identity: in message 3, initiator sends identity, and proof of knowledge of the shared key, encrypted with the Diffie-Hellman key. In message 4, the target sends its identity and proof of knowledge of the shared key encrypted with the Diffie-Hellman key.**
- **variant in which active attacker can learn target's identity: message 2 consists of Diffie-Hellman number and, encrypted with the Diffie-Hellman key, the target's identity and proof of knowledge of shared key. Message 3 is as in previous bullet.**

3. Suppose Alice is sending packets to Bob using IPsec. Suppose Bob's TCP acknowledgment gets lost, and Alice's TCP, assuming the packet was lost, retransmits the packet. Will Bob's IPsec implementation notice that the packet is a duplicate and discard it?

   No. IPsec treats a retransmitted TCP packet as a new IPsec packet. It is up to TCP to notice the packet is duplicate.

4. Would it be possible for the SA to be defined only by the destination address and the SPI (i.e., leave out whether it's ESP or AH)? Would this require any changes to the IPsec protocol? Would an implementation of a receiver that defined the SA based solely on destination address and SPI interwork with one that did what the IPsec specification says?

   Yes to both questions. Since it's the receiver that defines the SPI, it can assign different SPIs to ESP SAs vs. AH SAs. This will interwork with implementations that allow the same SPI to be assigned to both, and distinguish which SA it belongs to based on whether it's AH or ESP.

5. When sending encrypted traffic from firewall to firewall, why does there need to be an extra IP header? Why can't the firewall simply encrypt the packet, leaving the source and destination as the original source and destination?

   Suppose one portion of your Intranet is connected to the Internet with firewall F1, and another portion of your Intranet is connected with firewalls F2 and F. All addresses inside that portion are reachable equally well through F2 and F3. Since SAs are pairwise, F1 will have two SA's: one to F2, and one to F3. When F1 forwards, a packet for destination D, it has to choose which SA to send it on, encrypting the packet with the key for the F1-F2 SA or with the key for the F1-F3 SA. Internet routing can route packets for D via either F2 or F3. If it chooses a different F than F1 assumed, then it will not work. So F1 has to specify which of the F's the Internet should deliver the packet to.

6. Referring to Figure 17-2, assume that A and B are using IPsec in transport mode, and F1 and F2 have established an encrypted tunnel using IPsec. Assume A sends a TCP packet to B. Show the relevant fields of the IP header(s) as given to A's IP'sec layer, as transmitted by A, as transmitted by F1, and as received by B.

As given to IPsec layer: SOURCE=A, DESTINATION=B
As transmitted by A: SOURCE=A, DESINATION=B, PROTOCOL=ESP(or AH), ESP header NEXT HEADER=TCP
As transmitted by F1: starting from the outer header, SOURCE=F1, DESTINATION=F2, PROTOCOL=ESP, ESP header NEXT HEADER=IP; inner IP header exactly as transmitted by A
As received by B: exactly as sent by A

7. Suppose if Alice's aggressive-mode IKE connection initiate is refused, Alice starts up another aggressive-mode connection initiate with her next (and weaker) choice of Diffie-Hellman groups. What is the vulnerability, given an active attacker? (See §18.5.1 Aggressive Mode and Main Mode)

   The active attacker can trick Alice into using weak crypto. The bad guy can impersonate Bob and refuse Alice's strong crypto proposal. Then Alice will retry with a weaker proposal.

8. Show how someone who knows both Alice's and Bob's public encryption keys (and neither side's private key) can construct and entire IKE exchange based on public encryption keys that appears to be between Alice and Bob.

   Let trudy be the person attempting to construct an IKE exchange that looks like it's between Alice and Bob. For all IKE public encryption variants, the following applies. Trudy chooses Diffie-Hellman numbers a and b for each side, and nonces for each side. The proof of identity is a function of the other side's nonce (which ordinarily would require knowledge of one's private key since it is transmitted encrypted with the public key, but in this case Trudy has chosen the nonce and therefore knows it), the Diffie-Hellman values, and the cookies, all of which Trudy knows. Trudy can also compute the session keys, since she knows all the inputs, including $g^{ab} \mod p$, since she knows both a and b.

9. For Photuris, and for each of the Phase 1 IKE variants, say how it performs on hiding endpoint identifiers. Does it hide the initiator's and/or the responder's IDs from eavesdroppers? How about active attackers? (Hint for one tricky case: what are the implications if Alice sends the hash of Bob's certificate as she can optionally do in the public encryption variants?)

   Photuris: hides both from passive attackers. Hides Bob's from active attackers since Alice has to divulge and prove her identity first.
   IKE public signature key, main: both hidden from passive attackers. Hides Bob's from active attackers since Alice to divulge and prove her identity first.
   IKE public signature key, aggressive: neither hidden from passive or active attacker.
   IKE public encryption key, main, and aggressive: both hidden from passive as well as active attacker. If Alice sends the hash of Bob's certificate, then she leaks his identity to an attacker who has a list of possible recipients and their keys.

10. In the public encryption key case, SKEYID is defined as hash (nonces, cookies). SKEYID is supposed to be something that is not computable except by Alice and Bob. Why can't an

eavesdropper or active attacker calculate SKEYID?

Because the nonces are encrypted with the public keys of Alice and Bob (one is encrypted with Bob's public key, the other with Alice's and you need to know both in order to compute SKEYID).