

Set of Problems 2

Dr. Arjan Durrezi
Louisiana State University
Baton Rouge, LA 70810
Durrezi@csc.LSU.Edu

These slides are available at:

http://www.csc.lsu.edu/~durrezi/CSC4601_07/

Problem 1

- Suppose Alice is sending packets to Bob using IPSec. Suppose Bob's TCP acknowledgement 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?

Problem 1 - Solution

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

Problem 2

- ❑ 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 the destination as the original source and destination?

Problem 2 - Solution

- Because the real address could be reached through various farewalls.

Problem 3

- In IPSec when two transport mode SA are bundled to allow both AH and ESP protocols on the same end-to-end flow, only one ordering of security protocols seems appropriate: performing the ESP protocol before performing the AH protocol. Why is this approach recommended rather than authentication before encryption?

Problem 3 - Solution

- This order of processing facilitates rapid detection and rejection of replayed or bogus packets by the receiver, prior to decrypting the packet, hence potentially reducing the impact of denial of service attacks. It also allows for the possibility of parallel processing of packets at the receiver, i.e., decryption can take place in parallel with authentication.

Problem 4

- 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 group, rather than starting a main-mode exchange telling Bob all her supported Diffie-Hellman groups. What is the vulnerability, given an active attacker?

Problem 4 - Solution

- Alice could be actually be communicating with an attacker and not realize it. If she continues to pass the cryptographic algorithms she supports along with her weaker Diffie-Hellman groups, then she is exposing herself and compromising her security devices.

Problem 5

- ❑ What are the relative advantage of following key types as basis for an authentication exchange?
 - ❑ a) Pre-shared secret key
 - ❑ b) Public signature keys
 - ❑ c) Public encryption keys

Problem 5 - Solution

- ❑ a) Pre-shared secret key
 - Pre-shared keys often offer higher performance and are generally easier to configure.
- ❑ b) Public signature keys
 - It does not require one party to know the other party's public key before an exchange is initiated.
- ❑ c) Public encryption keys
 - It is possible for both sides to reveal their identity only to the person that they intended to authenticate themselves with.

Problem 6

- 16.2 Design a protocol in which Bob chooses whether to require Alice to send a cookie.

Problem 6 - Solution

- If Bob wants a cookie, have Bob reply to a message without a cookie with a "try again, this time returning this "cookie".

Problem 7

- Design a variant of Kerberos in which the conversation between Alice and Bob can have perfect forward secrecy.

Problem 7 - Solution

- Use the key in the Kerberos ticket to do a shared secret mutual authentication PFS protocol. For instance, do a Diffie-Hellman exchange, and have the session key be a function of the key in the ticket and the Diffie-Hellman key.