

Homework 5  
Due on April 26, 2007

Problem 1.

The IPSec architecture documents states that 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 2.

Consider the following threats to web security and describe how each is countered by a particular feature of IPSec.

- a. Brute force cryptanalytic attack. An exhaustive search of the key space for a conventional encryption algorithm.
- b. Known plaintext dictionary. Many messages will have predictable plaintext such as HTTP GET command. An attacker can construct a dictionary containing every possible encryption of the known plaintext message. When an encrypted message is intercepted, the attacker takes the portion containing the encrypted known plaintext and looks up the ciphertext in the dictionary. The ciphertext should match against an entry that was encrypted with the same secret key. This attack is especially effective against small key sizes (e.g. 40-bit keys).
- c. Replay attack. Earlier SSL handshake messages are replayed.
- d. Man in the middle. An attacker interposes during key exchange, acting as the client to the server and a server to the client.
- e. Password sniffing. Passwords in HTTP or other application traffic are eavesdropped.
- f. IP spoofing. Uses forged IP addresses to fool a host into accepting bogus data.
- g. IP hijacking. An active, authenticated connection between two hosts is disrupted and the attacker takes the place of one of hosts.
- h. SYN flooding. An attacker sends TCP SYN messages to request a connection but does not respond to the final message to establish the connection fully. The attacker TCP module typically leaves "half-open connections" around for a few minutes. Repeated SYN messages can clog the TCP module.