
Question 1

- (a) Is it possible to encapsulate an AH packet within an ESP packet and vice versa? Explain with the help of examples.
- (b) 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?
- (c) 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 IPsec layer, as transmitted by A, as transmitted by F1, and as received by B.
- (d) Why is IPsec not firewall-friendly?

Question 2

- (a) Why does the HMAC computation in SSL data transfer phase use a sequence number with each record even though SSL is built on top of TCP that delivers data in the correct order?
- (b) This question pertains to 3G-UMTS security. Consider the case when a user visits another country and turns her phone on to make a phone call and notices service X. However, it is possible that service provider X is actually service provider Y that charges a lot more for phone calls made while roaming. The service provider Y when working as the intermediary between the subscriber and the user's home network appears to be X to the user by stays as Y for the home network. How does the home network ensure that the user knows the service provider it is actually connecting to?
- (c) What are two advantages of computing the response to the challenge in the SIM card for GSM authentication?
- (d) What are two problems in deploying DDoS prevention solutions close to the sources of attack traffic?
- (e) Could the Local Aggregate Congestion Control mechanism for DDoS prevention result in collateral damage? Explain your answer.
- (f) Would it make sense to use crypto cookies in conjunction with IP traceback? Explain briefly.
- (g) What is a bloom filter? How could it be used to filter IP packets?

(h) Why doesn't the Botz-for-sale system use only one TCP connection to send the puzzle and receive the response instead of using two TCP connections?

(i) Why does it make sense to use an onion that encrypts information using public keys in the connection set up phase but secret keys during data movement?

Question 3

(1) What are the advantages of building security at the TCP layer?

(2) What flexibility does TCPsec provide for encrypting the TCP segment?

(3) How does TCPsec interoperate with NATS?

(4) Why does TCPsec handshake perform better than SSL?

References

- [1] S. Jana and S. K. Kasera. On fast and accurate detection of unauthorized access points using clock skews. In *ACM MOBICOM Conference*, Sept. 2008.
- [2] A. Psztor and D. Veitch, PC based precision timing without GPS, *SIGMETRICS Perform. Eval. Rev.*, vol. 30, no. 1, pp. 110, 2002.