COMP2190 – Semester 1 2020/2021

Tutorial 8

Problems

1. Discuss the opportunities for eavesdropping in any of the following scenarios. Consider software, hardware, network-based, and electronic means.
    a. Alice visits her friend, Bob's office. While she is there, she sits down at Bob's computer and uses it to access the uwimona.edu.jm WebMail server. To use WebMail, Alice needs to enter her username and password, which are sent over an SSL-protected link to the Web server.
    b. Ali takes his laptop to Café Blue to enjoy some coffee and free Wi-Fi wireless net access. He uses `telnet` to log in to his Linux machine back at home.

2. Suppose Alice sends packets to Bob using TCP over IPsec. If the TCP acknowledgement from Bob is lost, then the TCP sender at Alice's side will assume the corresponding data packet was lost, and thus retransmit the packet. Will the retransmitted TCP packet be regarded as a replay packet by IPsec at Bob's side and be discarded? Please briefly explain your answer.

3. Suppose an organization uses VPN to securely connect its sites over the Internet. Jim, a user in the organization, uses the VPN to communicate with his boss, Mary. Describe one type of communication between Jim and Mary which would not require use of encryption or other security mechanism, and another type of communication which would require encryption or other security mechanisms. Explain your answer.

4. A few years ago some people began to "sign" their email by including, at the bottom of an otherwise normal email message, the sender's name and the date encrypted in the sender's private key. The message itself is unencrypted, but the signature can be validated by using the finger command to retrieve the sender's public key. (Finger is an old utility for getting basic information about a user. If I run the command:
    `> finger userID@linux.uwimona.edu.jm`
    my local machine will send a message to a well-known port on the machine `linux.uwimona.edu.jm` where the finger daemon will respond with the contents of the file `.finger` from the user userID's home directory. So, users in this problem would just store their public key in their finger file.) Explain why this gives a completely false sense of security, by outlining 5 different ways that you could make it appear that the sender signed mail saying "Dr. Smith is a jerk." The definition of "different" is that each attack has a unique fix. For each of the five attacks you list, give a countermeasure that the sender/receiver could take to protect themselves against just that one attack, where the countermeasure would not help against any of the other attacks you list. You may assume that the sender and receiver are on different

machines, that both are running on "diskless" workstations whose files are provided by NFS, and that you have the ability to spy on and/or alter packets on any network at the sender or receivers site. However, you do not have the power to break into either the sender or receiver's machine | you can just view/change network packets.
Hint: You may find it helpful to draw a picture showing the flow of network messages in the system.

5. Give one reason why a firewall might be configured to inspect incoming traffic. Give one reason why it might be configured to inspect outgoing traffic. Do you think the inspections are likely to be useful?

6. 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?

7. Why isn't the SPI value sufficient for the receiver to know which SA the packet belongs to?

8. Suppose Alice wants to communicate with Bob using symmetric key cryptography using a session key K_S. Suppose that there is a key distribution center (KDC). The KDC is a server that shares a unique secret symmetric key with each registered user. For Alice and Bob, denote these keys by K_{A-KDC} and K_{B-KDC}. Design a scheme that uses the KDC to distribute K_s to Alice and Bob. Your scheme should use three messages to distribute the session key: a message from Alice to the KDC; a message from the KDC to Alice; and finally a message from Alice to Bob. The first message is $K_{A-KDC}(A, B)$. Using the notation K_{A-KDC}, K_{B-KDC}, S, A, and B answer the following questions:
    a. What is the second message?
    b. What is the third message?

9. Suppose you have an internal network with addresses from the 222.22/16 block. Provide a filter table and a connection table for a stateful firewall that is as restrictive as possible, but accomplishes the following:
    a. Allows all internal users to establish Telnet sessions with external hosts.
    b. Allows external users to surf the company web site at 222.22.0.12
    c. But otherwise blocks all inbound and outbound traffic.

    In your solution, suppose that the connection table is currently caching three connections, all from inside to outside. You'll need to invent appropriate IP addresses and port numbers.

Acknowledgment

1. Problem 1 is modified from a Problem Set by Prof. Ronald L. Rivest.
2. Problem 2 comes from a Homework Set at Vanderbilt University.
3. Problem 4 comes from a mid-semester test by Mike Dahlin.

4. Problems 3 and 5 come from “Computer Networks,” 5/E by A. S. Tanenbaum and D. J. Wetherall.
5. Problems 6 and 7 come from “Network Security: Private Communication in a Public World”, 2/E by C. Kaufman, R. Perlman, and M. Speciner.
6. Problems 8 and 9 come from “Computer Networking: A Top-Down Approach,” 7/E by J. F. Kurose and K. W. Ross.