CS 161 Fall 2006 — Computer Security Joseph/Tygar — HW 2

Due Friday, October 27 at 3pm

Please include the following at the top of the first page of your homework solution:

Your full name
Your login name
The name of the homework assignment (e.g. hw3)
Your TA's name and section number/time
Names of students you worked with

Please explain all work clearly. Your answers should be as concise as possible while still being complete and unambiguous.

Staple all pages together and put them in the CS 161/Fall 2006 slot of drop box #2 in 283 Soda. *No credit will be given after 3pm on the due date. If you have not finished, turn in what you have for partial credit.*

Homework exercises:

1. **(20 pts.) A Cryptographic Protocol**

   Suppose that someone suggests the following way to securely confirm that the two of you are both in possession of the same secret key. You create a random bit string the length of the key, XOR it with the key, and send the result over the channel. Your partner XORs the incoming block with the key and sends it back. You check, and if what you receive is your original random string, you have verified that your partner has the same secret key. Is this scheme secure?

2. **(20 pts.) RSA Eavesdropping**

   An RSA public-key is a pair (n,e) where $n = pq$ is the product of two primes.

   $RSA_{n,e}(m) = m^e \bmod n$

   Alice, Bob, and Carol use RSA public-keys $(n_A, 3)$, $(n_B, 3)$, and $(n_C, 3)$, respectively. David wants to send the same message m to the three of them. So David computes

   $$\begin{aligned} y_A &= m^3 \bmod n_A \\ y_B &= m^3 \bmod n_B \\ y_C &= m^3 \bmod n_C \end{aligned}$$

   and sends the ciphertexts y_i to the respective users.

   Show how an eavesdropper Eve can now compute the message m even without knowing any of the secret keys of Alice, Bob, and Carol.

3. (20 pts.) Secure PIN Entry

We want to allow a user to enter a secure PIN (numeric password) into a terminal. We assume that an adversary can monitor any input (such as a keyboard or keypad) but that the channel of the display to the user (such as a screen) is secure — the adversary cannot monitor it. Give a secure way for the user to enter his or her PIN (the adversary should gain no information about the PIN).

4. (20 pts.) Firewalls and Reference Monitors

Explain how the requirements of a reference monitor apply specifically to a firewall. Address the feasibility of determining whether a real firewall meets these requirements.

5. (20 pts.) Intrusion Detection Systems

Explain succinctly the difference between rule-based intrusion detection and statistical anomaly detection. Give one advantage each has over the other.