CS5285: Information Security for eCommerc Autumn, 2024
Tutorial 10, Week 12 (November 26) Gerhard Hancke

Questions:

1. **Firewall**

   (a) Consider a stateless firewall which allows company employees to connect to the Internet on ports 80 (HTTP), 443 (HTTPS) and 25 (SMTP, eMail). Fill out the table below with the rules necessary for this setup (use "outside" and "inside" for source and destination IP), do not forget to add a default rule at the end (7 rules in total).

Source IP	Dest. IP	Source Port	Dest. Port	Action

2. **Malware (1)**
   In each of the following scenarios, identify the type of malicious program that a host is being attacked by.

   (1) A program replicates itself in a very fast pace and severely slows down the host.

   (2) A program starts erasing data in a hard drive when the date becomes April 1st while the program does not infect any executable files.

   (3) A program emails a copy of itself to a subset of email addresses obtained from an address book stored in the host and starts erasing data in a hard drive when the date becomes April 1st.

   (4) A program monitors all HTTP GET messages sent out from the host and emails a copy of the messages to *trapdoor@whatever.email.net*.

3. **Malware (2)**

   (a) What is the difference between a virus and a worm?

   (b) Which kind of firewall could stop malware from spreading?

   (c) What are common defenses against malware?

   (d) Consider the following fragment in an authentication program. What type of malicious software is this?

```
username = read_username();
password = read_password();
if username is "122t-h4ck0r"
return ALLOW_LOGIN;
if usernmae and password are valid
return ALLOW_LOGIN
else return DENY_LOGIN
```

4. **TLS/SSL** Consider the protocols shown below (with $K = h(S, R_A, R_B)$):

$$\begin{array}{llllll} 1. & A & \rightarrow & B & : & R_A \\ 2. & A & \leftarrow & B & : & \text{Cert}_B,\ R_B \\ 3. & A & \rightarrow & B & : & \{S\}_B, E(K, h(msgs \mid\mid K)) \\ 4. & A & \leftarrow & B & : & h(msgs \mid\mid K) \\ 5. & A & \leftrightarrow & B & : & \text{Data encrypted under } K \end{array}$$

   (a) What would TLS look like if it was based on symmetric cryptography only? Would it be practical?

   (b) What is the purpose of the message $E(K, h(msgs \mid\mid K))$ sent in step 3?

   (c) If we remove this part in step 3, i.e., if we changed step 3 to

$$3. \quad A \quad \rightarrow \quad B \quad : \quad \{S\}_B$$

   Would the protocol still be secure?

5. **IKE (1)** Imagine you have a key exchange protocol similar to main mode in IKE Phase 1, but adding an additional piece of data ("cookies", C_A and C_B) to the message flow:

$$\begin{array}{llllll} 1. & A & \rightarrow & B & : & \text{CP, C}_A \\ 2. & A & \leftarrow & B & : & \text{CS, C}_A, \text{C}_B \\ 3. & A & \rightarrow & B & : & g^a \bmod p, R_A, \text{C}_A, \text{C}_B \\ 4. & A & \leftarrow & B & : & g^b \bmod p, R_B, \text{C}_A, \text{C}_B \\ 5. & A & \rightarrow & B & : & \text{E(K, ``Alice'' } \mid\mid \text{ proof}_A) \\ 6. & A & \leftarrow & B & : & \text{E(K, ``Bob'' } \mid\mid \text{ proof}_B) \\ 7. & A & \leftrightarrow & B & : & \text{Data encrypted under } K \end{array}$$

   The cookies are in the form

$$C_x = h(K_x, \text{IP}_{peer}, \text{timestamp})$$

   where K_x is a secret key only known to the party creating the cookie and IP_{peer} is the IP address of the peer (i.e., Alice would put Bob's IP and vice versa).

   (a) What are the reasons for including such cookies in the exchange?

   (b) The function of these cookies has to be effective before the exchange reaches step 5, otherwise B could be in trouble. Can you explain why?