Introduction to Computer Security, exercise 4, February 14-18, 2011

1. The Advo company built a Security Management System (SMS) and all the units of the company where connected to the Security Control Center (SCC) with the help of this management system. SCC was in the data center of the headquarters. In the same data center there were 30-40 other servers that took care of emails, Internet connections and other non-critical applications.

   Every unit had two serves that took care of emails and office applications. In every floor of every unit there were a PC which was used by the employees in order to connect to the internal network of the company and to Internet.

   Outline practices and actions with which SMS and the internal network can be protected.

2. A company C has hired the computer security firm of S to audit their networks. The analyst from S arrives and produces an USB memory. She states that the USB is to be loaded onto a system on the internal network. She will then run the program. It will scan the C's networks and send the information to S' headquarters. There, S analysts will determine whether the C's security is acceptable, and will recommend changes.

   a) The analyst informs C that the program works by sending the data to S' headquarters over the Internet using a proprietary protocol. She requests that the firewalls be opened to allow communincations to remote hosts with destination port 80. The audit department manager, who was told to hire S, is nervous. Should his security expert recommend that the communication be allowed, or not? Why?

   b) The analyst is asked exactly what the program does. She assures C that it does nothing harmful. Given that she is so vague, the C security officers want to find out more information. Suggest four or five questions that they should ask to obtain the information they seek.

   c) The analyst admits that her answers are based on what the S auditors have told her. When asked for the source code of the program in the USB, she states that it is proprietary and cannot be released. What could C's officers do to assure themselves that the program is not harmful?

   d) Based on the actions of the analyst, and assuming the finances are not a consideration, would you hire S to analyze your network security? Why or why not?

3. Suppose a message m is divided into blocks of length 160 bits: $m = M_1||M_2||\cdots||M_k$. Let $h(m) = M_1 \oplus M_2 \oplus \cdots \oplus M_k$ ($\oplus$ is the xor operation). Which of the properties a) quickly calculated, b) preimage resistance, c) collision resistance does h satisfy?

4. Assume that an old encryption method is used two times in order to increase the key size:

$$C = E_{k_1}(E_{k_2}(M)).$$

Now the size of keys is $|k_1| + |k_2|$. Let us assume that you know a plaintext-ciphertext pair. Show how you can find the secret key (k_1, k_2) without systematically going through all the key pairs.

5. Consider the following simplied version of the CFB mode. A plaintext is broken into 32-bit pieces $P = [P_1, P_2, \cdots]$, where each P_i has 32 bits rather than 8 bits used in CFB. Encryption proceeds as follows: An initial 64 bit X_1 is chosen. Then for $j = 1, 2, 3, ...$, the following is performed:

$$\begin{aligned} C_j &= P_j \oplus L_{32}(E_K(X_j)), \\ X_{j+1} &= R_{32}(X_j)||C_j, \end{aligned}$$

where $L_{32}(X)$ denotes the 32 leftmost bits of X, $R_{32}(X)$ denotes the rightmost 32 bits of X, and $X||Y$ denotes the string obtained by writing X followed by Y.

a) Find the decryption algorithm.

b) The ciphertect consists of 32-bit blocks $C_1, C_2, C_3, C_4, ...$ Suppose that a 1-bit transmission error causes C_1 to be received incorrectly. How many blocks are affected by this error and in what way?