Introduction to Computer Security, exercise 4, April 19-23, 2010

1. Research Chief Mikko Hyppönen from F-Secure will come to give a talk on Fight Against Network Criminality, on Wednesday April 14, at 14 o'oclock, in A 111. Although the talk in probably inb Finnish, the the lecture slides will appear in English on the home page of our course. Make a summary of the talk.

2. In the course, we have studied some file operations. In addition, explain the following Unix commands:

   a) chown and chgrp, and option -h

   b) tar and options -c, -r, -u, -t, -x

   c) file and options -c, -h, -m mfile

3. 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 finaces are not a consideration, would you hire S to analyze your network security? Why or why not?

4. 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 1) quickly calculated, 2) preimage resistance, 3) collision resistance does h satisfy?

5. An old DES-MAC cryptographic hash function would generate collisions given 2^{32} messages. Alice wants to take advantage of this to swindle Bob. She draws up two contracts, one that Bob has agreed to sign and the other that Bob would not sign. She needs to generate a version of each that has the same checksum. Suggest how she might do this. (Hint: Adding blank spaces, or inserting a chacter followed by a backspace, will not affect the meaning of either contract.)