Homework 4

Due: May 25, 2018 at 11:59pm **Extended; due date is now May 30** **Points:** 100

Questions

Remember to justify your answers.

1. (*40 points*) A company called the Drib has hired the computer security firm of Dewey, Cheatham, and Howe to audit their networks. The analyst from DC&H arrives and produces a floppy disk. She states that the disk is to be loaded onto a system on the internal network. She will then run the program. It will scan the Drib's networks and send the information to DC&H's headquarters in Upper Bottom. There, DC&H analysts will determine whether the Drib's security is acceptable, and will recommend changes.

   (a) The analyst informs the Drib that the program works by sending the data to DC&H's headquarters over the Internet using a proprietary protocol. She requests that the firewalls be opened to allow communications to remote hosts with destination port 80. The audit department manager, who was told to hire DC&H by the Drib's CEO, 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 the Drib that it does nothing harmful. Given that she is so vague, the Drib 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 DC&H auditors have told her. When asked for the source code of the program on the floppy, she states that it is proprietary and cannot be released. What could the Drib's officers do to assure themselves that the program is not harmful?

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

2. (*10 points*) As encryption conceals the contents of network messages, the ability of intrusion detection systems to read those packets decreases. Some have speculated that *all* intrusion detection will become host-based once all network packets have been encrypted. Do you agree? Justify your answer. In particular, if you agree, explain why no information of value can be gleaned from the network; if you disagree, describe the information of interest.

3. (*30 points*) The designers of the original UNIX password hashing algorithm used a 12-bit salt. Consider a system with 2^{24} users. Assume that each user is assigned a salt from a uniform random distribution and that anyone can read the password hashes and salts for the users.

   (a) What is the expected time to find all users' passwords using a dictionary attack?

   (b) Assume that eight more characters were added to the password and that the hashing algorithm were changed so as to use all 16 password characters. What would be the expected time to find all users' passwords using a dictionary attack?

   (c) Assume that the passwords were eight characters long but that the salt length was increased to 24 bits. Again, the salts (and the corresponding algorithms) are known to all users. What would be the expected time to find all users' passwords using a dictionary attack?

4. (*20 points*) Consider Multics procedures p and q. Procedure p is executing and needs to invoke procedure q. Procedure q's access bracket is (5, 6) and its call bracket is (6, 9). Assume that q's access control list gives p full (read, write, append, and execute) rights to q. In which ring(s) must p execute for the following to happen?

   (a) p can invoke q, but a ring-crossing fault occurs.

   (b) p can invoke q provided that a valid gate is used as an entry point.

   (c) p cannot invoke q.

   (d) p can invoke q without any ring-crossing fault occurring, but not necessarily through a valid gate.