

Information Assurance: Homework 4

Due October 10, 2007

1. In class we discussed a number of different types of separation to protect different entities from one another.
 - a. Describe one advantage and one disadvantage to physical separation.
 - b. Describe one advantage and one disadvantage to temporal separation.

2. For each of the memory protection frameworks below answer the following questions:
 - a. Does it protect the operating system from errors in the user process? How?
 - b. Does it protect one user process from another? How?
 - c. What is the limitation of this approach, if any?

The memory protection frameworks are:

- Fence register
- Base bounds registers
- Segmentation
- Paging
- Paged Segments

3. Consider the following system. There are the following users
 - Alice and Bob are Engineers
 - Carol is in Finance
 - Dave and Bob are system administrators
 - Ellen is the CEO

There are the following files:

- System designs which should be read and written by the Engineers and read by the CEO.
- Financial statements which should read and written by the Financial department and read by the CEO.
- System config files which should be read and written by the system administrators
- In an emergency, the CEO should be able to read and write all files and delegate access to others.

- a. Write an Access Control Matrix for this system
 - b. Write access control lists for the representative types of objects that encodes these constraints.
 - c. Write capabilities for the users that encode these constraints.
4. A system allows the user to choose a password with a length of one to ten characters inclusive. Assume that 15,000 passwords can be tested per second. The system administrators want to expire passwords once they have a probability of 0.10 of being guessed. Determine the expected time to meet this probability under each of the following conditions.

- a. Password characters must be digits (“0” through “9”).
 - b. Password characters may be capital letters (“A” through “Z”) and numerics (“0” through “9”).
 - c. 12 bits of salt are added for both a and b.
5. Try running the John the Ripper password cracking program <http://www.openwall.com/john/>. You should be able to install it local to your environment for an unprivileged account. Obtain a password file from <http://www.cs.uiuc.edu/class/fa07/cs461/class07-passwd> This file contains nine accounts with passwords from a linux system. At least one password should be cracked very easily. If you have access to a private system, try running the program for a while longer to see if you get more passwords cracked. Submit the account names and passwords that you crack. As long as you get the quickly cracked passwords, you will get full credit.
6. An organization implements a biometric authentication system. All employees register their fingerprints, and the organization stores the resulting templates on a central server. Eve hacks the server and gains access to the template. What harm can occur from this breach? How does it compare to hacked passwords?