CE4062/CZ4062 Computer Security

Tutorial 5 – Operating System Security (1)

1. Answer the following questions
   a. Give an example of how a rootkit can compromise the system after obtaining the root privilege.

   b. Briefly describe three stages employed by the OS.

   c. What is the controlled invocation? What is its potential danger?

2. Consider a computer system with three users: Alice, Bob, and Cindy. Alice owns the file *alicerc*, and Bob and Cindy can read it. Cindy can read and write the file *bobrc*, which Bob owns, but Alice can only read it. Only Cindy can read and write the file *cindyrc*, which she owns. Assume that the owner of each of these files can execute it.
   a. Create the corresponding access control matrix.

   b. Cindy gives Alice permission to read *cindyrc*, and Bob removes Alice's ability to read *bobrc*. Show the new access control matrix

   c. Show the capabilities associated with Alice.

3. Let's consider the scenario in Q2 again. Assume this is the Unix system. The users Bob and Cindy are in the same group, while Alice is in a different group.
   a. For the original access control matrix in Q2(a), please write the permission for the files *alicerc*, *bobrc* and *cindyrc*.

   b. To adjust the permissions in Q2(b), please write the corresponding commands for *cindyc* and *bobrc*, respectively.

4. A group of researchers is working on analyzing web search results from a major Internet search provider. At the Internet company, a group of search engineers collects and updates databases of: search queries, IP (internet protocol) addresses where the queries came from and timestamps for the queries made by online users. A search manager is in charge of the group of engineers, and can read the query and timestamps database, but not the IP address database -- due to privacy concerns. The researchers are able to access the databases with read-only privileges. The general public should not have access to the database for privacy reasons .
   a. Complete the access control matrix by filling in the access permissions for the different objects shown. Each entry can be either read, write, read/write, or '-' (for no access).

   b. List the ACLs for each object (or class of objects)

   c. List the capabilities for each subject (or class of subjects).