CS590U: Access Control: Theory and Practice Spring 2005

Assignment #3 Due: Tuesday, Feb 8, 2005.

Problem 1 This problem asks you to study the safety analysis problem in Unix. For simplicity, we assume that all files are under the root directory (there is no subdirectory) and that every user has rwx permission to the root directory. We consider only read/write access to the files within the root directory. Some elements of the UNIX access control system are as follows.

- There are the notion of groups. Each user is a member of a primary group and zero or more other groups.
- There is a superuser, who has access to everything. For the purpose of safety analysis, we will assume that the superuser is trusted, i.e., it does not initiate any action.
- A user can create a file, in which case the user is the owner of the file. A user can destroy a file if it has write permission to the file. Owner of a file can use commands such as `chown` to change ownership for the file, `chgrp` to change the group of a file, and `chmod` to change the access permissions of a file. For simplicity, we assume only the following possibilities for `chmod`: `chmod+r`, `chmod-r`, `chmodg+r`, `chmodg-r`, `chmodo+r`, `chmodo-r`, and six similar commands for the write right.

a. (25 pts) Build a state-transition system for Unix access control system, with the assumptions described above.

- Precisely define what are the sets, relations, and functions in each state.
- Write pseudo-code for determining whether a user has access to a file.
- Describes how the following command may change the state: `create_file`, `chown`, `chgrp`, `destroy_file`, `chmod-r`, `chmodg+w`, `chmodo-r`.

b. (20 pts) Formally define a safety analysis problem to address the following concern: one wants to know whether another particular user u can read a file f assuming users in a set T are trusted (i.e., users in T do not initiate any action). Find an efficient algorithm to solve the above problem, and give the computational complexity of the algorithm.

c. (20 pts) Now suppose that one wants to know whether whether u is and will always be the owner of a file f, assuming that users in T are trusted. Define an analysis problem for it and find an efficient algorithm to solve the problem, and give the computational complexity of the algorithm.

d. (20 pts) Now suppose that one wants to know whether a user u can learn information stored in a file f, assuming that users in T are trusted. Define an analysis problem for it and find the most efficient algorithm to solve the problem.

e. (5 pts) Comment on whether the HRU model and the known results are applicable to the above analysis problems.

Problem 2. (10 pts) In Section III of Anita Jones' article "Protection Machanism Models: Their Usefulness", Jones defines a model to be useful if it

1. accurately and concisely expresses the essence of the phenomena of interest, and
2. tells a system designer or user something he did not know or understand without the model.

Jones then go on to argue that the Take-Grant system accurately reflects the basic attributes of extant protection mechanisms. Do you buy the arguments she gave? Why or why not?