CS167 Homework Assignment 4

Due 11:59pm May 3, 2023

1. [33%] Tenex was an operating system for DEC PDP-10 computers used the late ’60s and early ’70s. It had a number of features, including one that allowed user process to provide functions to be invoked (in user mode) after each of its page faults. It stored passwords in plain text (i.e., unencrypted) in a file that was adequately protected. A user could supply his or her password not only when logging in, but also from a program so as to switch from one protection domain to another. The system code that checked for a correct password would do so one character at a time, moving from left to right, stopping when it encountered an incorrect character. It was soon discovered that in time proportional to the length of the password one could figure out any user’s password. Explain how.

2. [33%] In lectur ed protection domain
in Unix in whic n we will see if this
really is possib 19, or the textbook,
starting on pag

   Let’s assume th wned by PUB (except
for perhaps a fe UB any form of
access; and PU PUB user ID has
access only to f

   We’d like to cr a pathname of an input
file, a pathnam run that will be able
to read the inpu access to any other
files except for

   a. [11%] e/you/malware. The
progra stdin and write it to
stdout. using the command

      ```
      secur
      ```

      /home/ B). YOU has access to input and output, but PUB does not. Thus PUB shouldn’t have access to any of your other files.

      How can secureRun set its user ID to PUB, yet allow access to the files **input** and **output**? [Hint: it might be necessary for it to exec some other, intermediary, program that’s been set up in a special way.]

   b. [11%] Although the process is running as user ID PUB and has access to the files **input** and **output**, is it prevented from accessing other files you own? Explain.

   c. [11%] What else should be done to make sure /home/you/malware cannot do anything other than what you intend for it to do? [Hint: read the man page for **setreuid**.]

3. [34%] NFS v2 and v3 systems allow clients to “hard mount” remote file systems, so that in the event of a server crash (or network outage), clients repeatedly retry RPC calls until the server (or network) comes back up. If clients held locks on any of the server’s files, the network lock

manager (NLM) protocol recovers these locks for them. Note that if a client places a system call on a file in a hard-mounted file system, the system call will not fail with a time-out error, even if the server crashes and takes a long time to restart.

a. [17%] Assume that all RPC calls are to idempotent procedures and that the only possible failure is a server crash (i.e., clients don't crash and the network is well behaved). Other than timing issues, will server crashes have any adverse effects on clients (assuming the server comes back up)? Explain. You may assume that neither clients nor server are overloaded.

b. [17%] Now suppose all clients and servers are interconnected by a single network: it's either working and connecting all parties, or is down and is connecting none of them. It can switch from up to down or vice versa at any moment. Will it be the case that server crashes have any adverse effects on clients? Explain.