COMS W4187 Security Architecture and Engineering

Homework Assignment 2

1 Programming Assignment

1.1 A Homework Submission System

The assignment is to implement a simple homework submission system, which copies a student's file into some protected directory. To do this, you will need to use a virtual machine; see the details below.

So — write a program that simulates the submission operation (named as `hwsub`). It has to copy files to some protected directory. It also has to create a log file of each submission. Again, this log file must be protected against unauthorized viewing or modification. A student is allowed to submit homework more than once, but only the last copy will be stored in the submission directory. To assure the integrity of a submitted file, a MD5 checksum of that file will be displayed on the screen upon successful submission. Also, this checksum is recorded in the log file for future reference.

You also need to write programs that display one's submission record if any (named as `hwsubls`) and remove submitted files (named as `hwsubrm`). Naturally, only the owner is allowed to view his submission history, and over-write or remove his files. Again, maintain the log file properly upon these operations.

Deliverables:

1. Source code;
2. Test shell scripts that exercise the submission program;
3. A directory tree with all necessary directories and files used, with appropriate permissions;
4. A 1-2 page writeup explaining the security theory of your design. This will count as the written part of this assignment;
5. Besides submitting the usual tar file including everything, also leave a copy of homework in your VM. The TA will log in to your VM to test your program.

1.2 Virtual Machine

A virtual machine appears to be a complete computer, running some operating system; in fact, though, it is just an application running on some other computer. The advantage of using virtual machines (VMs) is that each user can have full privileges, including root privileges.

Instructions on using VMware are at
`http://www.cs.columbia.edu/~smb/classes/f08/vmware.pdf`

Initially, you will log in as root (you will receive the machine name and password). The first thing to do is to change the password to something else. Note carefully: your documentation MUST include the new password; the TAs will log in to your VM to test your code. Of course, this means that you SHOULD NOT use your normal password. Next, you'll have to create two or three logins:

```
/usr/sbin/useradd user1
/usr/sbin/useradd user2
```

etc. Create at least two user accounts — users who will try to use your submission system — plus an account for your programs to run under. To use one of these accounts, Instead of logging in as those users, it's easier to log in as root and then do

```
su user1
```

You may use either setuid or message-passing. I suspect that setuid is easier, since otherwise you need to learn some strange Linux primitives. That said, if you want to use message-passing, you're welcome to.

If you compile your program as the hwsub login, you can make it setuid by saying

```
chmod +s filename
```

If you compile it as root and you want it to run as, say, user hwsub, you must do

```
chown hwsub filename
chmod +s filename
```

Note well: when you're running as root, you have the potential to destroy part or all of the VM. In that case, you'll have to contact CRF to get it restored, and you'll probably lose any files you had created on the VM. Note that last point carefully: VMs have their own file system; you are well-advised to keep copies of all your work on your CS account's home directory.

2 Written Assignment

The written assignment for homework 2 is a security design document for the programming assignment. In it, you should explain the security decisions, designs, and features of your program.

First, what are the threats against which you're defending? Be specific — don't just recite the trilogy. What are the threats you are not defending against?

Second, explain how your program achieves those goals. For any files or directories you create, explain why you selected particular ownership and modes. What would happen with looser permissions? Tighter ones?

Third, explain the privileges used by any privileged programs. What are the privileges, how do they achive your goals, and how are the priviliges acquired by those programs?

Fourth, describe anything else relevant to the security properties of your program.

Last, as described in the programming assignment, give the information necessary for the TAs to test your code.

Don't waste time and space with routine statements about how security is important, what confidentiality is, etc. This isn't a report to upper management; it's a design document from one professional (you) to another (me) about a specific set of programs.

I believe that the length of the document will be 2-3 pages. Don't be alarmed if it's shorter; don't worry if it's longer unless it's a lot longer. I'm not concerned with "pretty", layout, fancy graphics, or diagrams unless those are necessary to explain things more clearly.