

Analyze the local and global impact of computing on individuals with respect to security

You may not collaborate with anyone on this assignment.

Background:

1. **SUID** (Adapted from *Practical UNIX Security*)

Sometimes it's necessary for unprivileged users to be able to accomplish tasks that require privileges. An example is the `passwd` program, which allows you to change your password. Changing a user's password requires modifying the `/etc/passwd` file. Users should not have access to change this file directly, however: a user could change everybody else's password as well!

To get around these problems, UNIX allows a program to be granted additional privilege. A process executing one of these programs can assume a different user ID (UID) while they are running. A program that changes its UID in this manner is called a SUID program (set user ID). When a SUID program is run, its effective UID becomes that of the *owner of the file*, rather than that of the user who is running it.

If a program is SUID the output of the `ls -l` command will show what is normally an `x` in the owner permissions as an `s`.

```
$ ls -l foo
-rwsr-xr-x root faculty 12345 Feb 26 2008 foo
```

In this case program `foo`, when run, will have the privileges of the *root* user (the *superuser* ... who has the ability to do anything on the system!). You should begin to see that this powerful mechanism is fraught with security dangers! Many security holes have been discovered by people who figured out ways of making a SUID program do something that it was not designed to do.

(As a side note, programs can also be made SGID (set group ID), where they assume the privileges of the *group owner* of the file while they are executing. For example, the `submit` program is SGID: when you run it the program assumes the privileges of the `faculty` group, which has permission to copy files into a directory owned by your instructor, something you do not have permission to normally do, not being a member of the `faculty` group)

2. **Open Source** In general, the term *open source* refers to any program whose source code is made available for use or modification as users or other developers see fit.

Scenario: The users of a UNIX system request that a certain SUID open source program be installed on the system for everyone's use. Let's say this code was written by Company X. The Systems Administrator installs the program, where it is used happily by most of the system's users. Unfortunately, one of the users on the system finds an exploit in the open source code and uses it to obtain root access on the system and destroy everyone's data.

Analyze the local and global impact of computing on individuals with respect to security

You may not collaborate with anyone on this assignment.

1. Who is to blame for this situation? Pick two and argue why it's their fault: Systems Administrator, Nefarious User, or Company X. Hand in your argument in a paper approximately two pages in length, typed, double-spaced, 12 point Times New Roman font, 1" margins. You should address the impact this set of events has on (a) the general users of the UNIX system, and (b) its impact on the organization that operates the UNIX system.

2. Read the following two reference documents. Add to your paper a list of the specific areas of these two documents that may have been violated, and state how.

References: *Acceptable Use Policy for USNA IT Resources*

intranet.usna.edu/IRC/policies/AcceptableUse.htm

System Administrator's Code of Ethics

www.sage.org/ethics/index.html

Assigned: Monday 03 March 2008
Due: Wednesday 05 March 2008
Discussion: Monday 17 March 2008

Important note: Completing this assignment is not optional: failure to complete and turn in this assignment will result in a course grade of "F".