

Laboratory 2

Due Date: May 23, 2008

Points: 100

When you download a program, or need to execute a program that you don't trust, you want to isolate the program as much as possible. One aspect of this is to ensure it runs with as few privileges as possible. Running it with privileges of no user will limit the program's ability to read, modify, create, and delete files. Specifically, if we give the program a UID that belongs to no existing user, then the program can read only those files that are world-readable, and modify only those files that are world-writeable.

The laboratory assignment is to modify the FreeBSD kernel to add a new system call. This call has the following interface:

```
int setuidprot(void);
```

When invoked, this call generates a number between 10,000 and 19,999 inclusive, sets the effective UID of the program to that value, and returns it as the value of the system call.

Your routine is to assign the first UID as 10000, the second as 10001, and so forth. If the last UID assigned was 19999, the next one assigned should be 10000.

For this lab, you can assume that no user has a UID in the given range.

To turn in: Please create a tar file containing the files you modify and a README describing the changes you made. Submit it to SmartSite.