

Homework 4

1. What does the principle of least privilege say?
2. In which of the following situations can the access control mechanism of Unix file permissions be used?
 - (a) Alice wants to have her files readable, except for her office mates.
 - (b) Bob and Sam want to share some secret files.
 - (c) Root wants some of her files to be public.
3. Explain what is meant by *Kerckhoffs' principle*.
4. How can a system that separates between *users* and *root* be of any help with buffer overflow attacks?
5. What does it mean that the program `passwd` has the `setuid` bit set? Why is this necessary?
6. With which permissions does the program `login` normally have and why is this needed?
7. The variable `PATH` is a shell variable in UNIX which lists all directories that should be automatically searched for a program. For example if `PATH` contains the directory `/usr/bin` and the program `ls` is stored there, then a user does not need to type `/usr/bin/ls` to run this file, but `ls` suffices. The question is why is it a bad idea in general, but in particular for `root`, to have `.` as the first entry in ones variable `PATH`?
8. A Unix directory might look as follows:

```
$ ls -ld . * */*
drwxr-xr-x 1 ping staff 32768 Apr  2 2010 .
-rw----r-- 1 ping students 31359 Jul 24 2011 manual.txt
-r--rw--w- 1 bob students 4359 Jul 24 2011 report.txt
-rwsr--r-x 1 bob students 141359 Jun  1 2013 microedit
dr--r-xr-x 1 bob staff 32768 Jul 23 2011 src
-rw-r--r-- 1 bob staff 81359 Feb 28 2012 src/code.c
-r--rw---- 1 emma students 959 Jan 23 2012 src/code.h
```

with group memberships assigned as follows:

Members of group staff: ping, bob, emma
Members of group students: emma

The file `microedit` is a text editor, which allows its users to open, edit and save files. Note carefully that `microedit` has set its `setuid` flag. Fill in the access control matrix below that shows for each of the above five files, whether `ping`, `bob`, or `emma` are able to obtain the right to read (R) or replace (W) its contents using the editor `microedit`.

	<code>manual.txt</code>	<code>report.txt</code>	<code>microedit</code>	<code>src/code.c</code>	<code>src/code.h</code>
<code>ping</code>					
<code>bob</code>					
<code>emma</code>					

9. In the context of which information flow should be protected, explain briefly the differences between the *read rule* of the Bell-LaPadula access policy and the Biba access policy. Do the same for the *write rule*.