

## Homework 4

Please submit your solutions to the email address 7ccsmen at gmail dot com. Please submit only one homework per email. Please also submit only ASCII text or PDFs. Every solution should be preceded by the corresponding question, like:

**Q<sub>n</sub>:**     ...a difficult question from me...  
**A:**        ...an answer from you ...  
**Q<sub>n</sub> + 1**   ...another difficult question...  
**A:**        ...another brilliant answer from you...

**Solutions will only be accepted until 20th December!**

1. What should the architecture of a network application under Unix be that processes potentially hostile data?
2. What is a unikernel system and why is a unikernel preferable on a web server system (in contrast to a traditional general purpose operating system like Linux). Hint: What is the idea of a unikernel?
3. What does the principle of least privilege say?
4. How can you exploit the fact that every night root has a cron job that deletes the files in /tmp? (Hint: cron-attack)
5. 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.
6. Explain what is meant by *Kerckhoffs' principle*.
7. How can a system that separates between *users* and *root* be of any help with buffer overflow attacks?
8. What does it mean that the program `passwd` has the `setuid` bit set? Why is this necessary?
9. Under Unix (for example BSD Unix, MacOSX) the `login` program has the `setuid` bit set. Why is this needed? In Linux `login` does *not* have the `setuid` bit set. What are the consequences of this choice?

10. 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?
11. 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.

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

12. 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*.
13. **(Optional)** This question is for you to provide regular feedback to me, for example what were the most interesting, least interesting, or confusing parts in this lecture? Please feel free to share any other questions or concerns.