Homework 3

- 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. What should the architecture of a network application under Unix be that processes potentially hostile data?
- 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. What does it mean that the program passwd has the setuid bit set? Why is this necessary?
- 6. Assume format string attacks allow you to read out the stack. What can you do with this information? (Hint: Consider what is stored in the stack.)
- 7. Assume you can crash a program remotely. Why is this a problem?
- 8. How can the choice of a programming language help with buffer overflow attacks? (Hint: Why are C-programs prone to such attacks, but not Java programs.)