Universität des Saarlandes
Lehrstuhl für Softwaretechnik
Prof. Andreas Zeller, Stephan Neuhaus
Design of Secure Software Systems
Exercise 6

Total number of points obtainable: 14, plus 2 bonus points.

1 Access Control

1.1 Funny Bits

(6 points) The following Unix permission bits were all found on a live Unix system. For every permission bit set, give an example when you would give permissions like these on a file or directory. The column named 'T' is for the file type: 'd' stands for directory, 'f' stands for regular file.

T	U	G	O	Owner	Group
d	`--x`	`--x`	`--x`	root	root
f	`rws`	`r-x`	`r-x`	root	root
f	`rwx`	`rws`	`r-x`	root	tty
d	`rwx`	`rws`	`---`	neuhaus	admin
d	`rwx`	`--x`	`--x`	neuhaus	users
f	`rwx`	`--x`	`--x`	neuhaus	users

Hint: Don't just read off the permission bits, i.e., don't just say "I want the file to be executable but not readable". Instead, give a practical example when it would be useful to give a file execute permission, but no read permission.

2 Policies

2.1 Chinese Wall Policy

The Chinese Wall policy works by partitioning objects into conflict-of-interest classes. Initially, a subject has access to all objects in a conflict of interest class. Once the subject commits to an object in a particular class, it can't get access to any other object in that class.

For this exercise, assume that the objects in a particular conflict class are employee records containing the employee's name and salary. Also assume that conflict classes can contain only objects, not object groups.

- **(2 points)** Show that the commitment to an object must be permanent; i.e., it must not be possible for a subject to revoke its commitment to an object.
- **(2 points)** Show that it is not possible to compute an average of all employee's salaries.
- **(4 points + 2 bonus points)** John Clever, a student, tried to solve this problem by putting each employee record in its own conflict-of-interest class. He would then be able to read all employee's salaries (but not their names) and compute an average. He then found out that he had to put the average salary in its own conflict class. (Explain why for 2 bonus points.) Then, describe how it is possible to violate the policy to infer an arbitrary employee's name *and* salary.