Homework 1

Due: October 16, 2014 **Points:** 100

Questions

1. (*10 points*) The aphorism "security through obscurity" suggests that hiding information provides some level of security. Give an example of a situation in which hiding information does not add appreciably to the security of a system. Then give an example of a situation in which it does.

2. (*30 points*) Consider the set of rights {*read*, *write*, *execute*, *append*, *list*, *modify*, *own*}.

   (a) Using the syntax in Section 2.3, write a command *delete_all_rights*(p, q, o). This command causes p to delete all rights the subject q has over an object o.

   (b) Modify your command so that the deletion can occur only if p has *modify* rights over o.

   (c) Modify your command so that the deletion can occur only if p has *modify* rights over o and q does not have *own* rights over o.

3. (*30 points*) The proof of Theorem 3.1 states the following: Suppose two subjects s_1 and s_2 are created and the rights in $A[s_1, o_1]$ and $A[s_2, o_2]$ are tested. The same test for $A[s_1, o_1]$ and $A[s_1, o_2] = A[s_1, o_2] \cup A[s_2, o_2]$ will produce the same result. Justify this statement. Would it be true if one could test for the absence of rights as well as for the presence of rights?

4. (*10 points*) Someone asks, "Since the Harrison-Ruzzo-Ullman result says that the security question is undecidable, why do we waste our time trying to figure out how secure the UNIX operating system is?" Please give an answer justifying the analysis of the security of the UNIX system (or any system, for that matter) in light of the HRU result.

5. (*20 points*) Suppose a user wishes to edit the file *xyzzy* in a capability-based system. How can he be sure that the editor cannot access any other file? Could this be done in an ACL-based system? If so, how? If not, why not?

Extra Credit

1. (*10 points*) Peter Denning formulated the principle of attenuation of privilege as "a procedure cannot access an object passed as a parameter in ways that the caller cannot." Contrast this formulation to that of the Principle of Attenuation of Privilege in Section 2.4.3. In particular, which is the "subject" and which is the "other subject" in the earlier statement?

2. (*20 points*) Prove that the set of unsafe systems is recursively enumerable.
   Hint: Use a diagonalization argument to test each system as the set of protection systems is enumerated. Whenever a protection system leaks a right,add it to the list of unsafe protection systems.