Homework #1

Due: January 20, 2011 **Points:** 100

Questions

1. (*20 points*) Companies usually restrict the use of electronic mail to company business but do allow minimal use for personal reasons.

   (a) How might a company detect excessive personal use of electronic mail, other than by reading it? *Hint:* Think about the personal use of a company telephone.

   (b) Intuitively, it seems reasonable to ban all personal use of electronic mail on company computers. Explain why most companies do not do this.

2. (*16 points*) Consider a system that allows multiple owners of an object. This system allows an owner to grant rights to other subjects, and to delete them, except that the owner cannot delete another *own* right.

   (a) An object o has two owners, p and q. What happens if p deletes all of q's rights to the object? Specifically, does this prevent q from accessing the object?

   (b) Assume there are two types of own rights, an "original own" own_{orig} and an "added own" own_{add}. The own right own_{orig} cannot be copied or added, whereas the own_{add} right enables the possessor to add or delete rights (except for the own_{orig} right). If p has own_{orig} and q has own_{add}, how does your answer to the first part change?

3. (*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 as stated in class ("A subject may not increase its rights, nor grant rights it does not possess to another subject"). In particular, which is the "subject" and which is the "other subject" in the formulation used in class?

4. (*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?

5. (*24 points*) Prove or disprove: The claim of Lemma 3.1 holds when $\mathbf{x}$ is an object.

Extra Credit

1. (*20 points*) Prove Theorem 3.3.
   Hint: Use a diagonalization argument to test each system as the set of protection systems is enumerated.