Homework #1

Due: April 12, 2013 **Points:** 100

Questions

1. (*20 points*) Consider a very high-assurance system developed for the military. The system has a set of specifications, and both the design and implementation have been proven to satisfy the specifications. What questions should school administrators ask when deciding whether to purchase such a system for their school's use?

2. (*16 points*) Let c be a copy flag and let a computer system have the rights {*read*, *write*, *execute*, *append*, *list*, *modify*, *own*}.

   (a) Using the syntax in Section 2.3, write a command *copy_all_rights*(p, q, s) that copies all rights that p has over s to q.

   (b) Modify your command so that only those rights with an associated copy flag are copied. The new copy should *not* have the copy flag.

   (c) In the previous part, what conceptually would be the effect of copying the copy flag along with the right?

3. (*10 points*) Minsky [1, p. 256] states that "privileges should not be allowed to grow when they are transported from one place in the system to another." Does this differ from the Principle of Attenuation of Privilege as stated in class? If not, show they are the same; if so, how do they differ?

4. (*30 points*) Prove Theorem 3.3. (*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.)

5. (*24 points*) Prove Lemma 3.2.

Extra Credit

1. (*20 points*) Prove or give a counterexample:
   The predicate *can•share*$(\alpha, \mathbf{x}, \mathbf{y}, G_0)$ is true if and only if there is an edge from $\mathbf{x}$ to $\mathbf{y}$ in G_0 labeled α, or if the following hold simultaneously.

   (a) There is a vertex with an **s**-to-**y** edge labeled α.

   (b) There is a subject vertex $\mathbf{x}'$ such that $\mathbf{x}' = \mathbf{x}$ or $\mathbf{x}'$ initially spans to $\mathbf{x}$.

   (c) There is a subject vertex $\mathbf{s}'$ such that $\mathbf{s}' = \mathbf{s}$ or $\mathbf{s}'$ terminally spans to $\mathbf{s}$.

   (d) There is a sequence of subjects $\mathbf{x}_1, \ldots, \mathbf{x}_n$ with $\mathbf{x}_1 = \mathbf{x}'$, $\mathbf{x}_n = \mathbf{s}'$, and $\mathbf{x}_i$ and $\mathbf{x}_{i+1}$ $(1 \leq i < n)$ being connected by an edge labeled t, an edge labeled g, or a bridge.

References

[1] Naftaly Minsky. The principle of attenuation of privileges and its ramifications. In Richard A. DeMillo, David P. Dobkin, Anita K. Jones, and Richard J. Lipton, editors, *Foundations of Secure Computing*, pages 255–277. Academic Press, New York, NY, USA, 1978.