Homework 1

Due Date: January 18, 2011 **Points:** 100

Questions

1. (*20 points*) The police and the public defender share a computer. What security problems does this present? Do you feel it is a reasonable cost-saving measure to have all public agencies share the same (set of) computers?

2. (*10 points*) Suppose Alice has *r* and *w* rights over the file *book*. Alice wants to copy *r* rights to *book* to Bob.

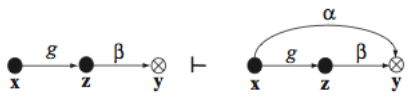
   (a) Assuming there is a copy right *c*, write a command to do this.

   (b) Now assume the system supports a copy flag; for example, the right *r* with the copy flag would be written as *r*:*c*. In this case, write a command to do the copy.

   (c) In the previous part, what happens if the copy flag is *not* copied?

3. (*20 points*) Naftaly Minsky said that "privileges should not be allowed to grow when they are transported from one place in the system to another." Is this the same as 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")? If so, *show* they are the same; if not, how do they differ?

4. (*20 points*) Prove Lemma 3.2, which says that, for a set of rights β and $\alpha \subseteq \beta$:



5. (*30 points*) Let *B* be the set of words associated with bridges, and *C* the set of words associated with connections. Prove the following theorem *in detail*: The predicate $can \bullet know(\mathbf{x}, \mathbf{y}, G_0)$ is true if and only if there exists a sequence of subjects $\mathbf{u}_1, \ldots, \mathbf{u}_n \in G_0$ ($n \geq 1$) such that the following conditions hold simultaneously:
   (a) $\mathbf{u}_1 = \mathbf{x}$ or $\mathbf{u}_1$ rw-initially spans to $\mathbf{x}$;
   (b) $\mathbf{u}_n = \mathbf{y}$ or $\mathbf{u}_n$ rw-terminally spans to $\mathbf{y}$;
   (c) For all i such that $1 \leq i < n$, there is an rwtg-path between $\mathbf{u}_i$ and $\mathbf{u}_{i+1}$ with associated word in $B \cup C$.
   Hint: Use induction on n.

Extra Credit

1. (*20 points*) Argue for or against the following proposition. Ciphers that the government cannot cryptanalyze should be outlawed. How would your argument change if such ciphers could be used provided that the users registered the keys with the government?