Homework 1

Due Date: January 26, 2009 **Points:** 100

Questions

1. (*10 points*) A respected computer scientist has said that no computer can ever be made secure. Why might she have said this? (*text*, problem 1.14)

2. (*20 points*) Consider a computer system with three users: Alice, Bob, and Cyndy. Alice owns the file *alicerc*, which she, Bob and Cyndy can read. Cyndy and Bob can read and write the file *bobrc*, which Bob owns, but Alice can only read it. Only Cyndy can read and write the file *cyndyrc*, which she owns. Also, assume the owner of each of these files can execute it.
   (a) Create the corresponding access control matrix.
   (b) Write a command *addapp* that allows a subject p to grant a (append) permission to a second user q for a file x if, and only if, p owns x and q has w permission for x.
   (c) Assume that the primitive operation "**enter** a **into** $A[s,o]$ is *disallowed*. This means it cannot be put into a command. The command *addapp* may be used. Is it possible for the system with initial state as described above to be in a state where Cyndy has a rights over *bobrc*, but not w rights over *bobrc*? Either give a sequence of commands that put it into that state, or prove that it cannot enter that state.
   (d) Write a command *delapp* that allows a subject p to delete a (append) permission to a second user q for a file x if, and only if, p owns x, q has a permission for x, and q has either r or w permission for x.

   (*text*, problem 2.1, modified)

3. (*20 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? (*text*, problem 3.1)

4. (*10 points*) Reverse the edge between **d** and **e** in Figure 3–4 so there is an edge labeled g from **d** to **e**. Is $can \bullet share(r, \mathbf{x}, \mathbf{z}, G_0)$ still true? If so, please show a witness; if not, please prove it does not hold.

5. (*40 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. (*40 points*) Devise an algorithm that determines whether or not a system is safe by enumerating all possible states. Is this problem *NP*-complete? Justify your answer. (*text*, problem 3.2)