Homework 1

Due Date: April 20, 2000
Points: 100

1. (*10 points*; handout, exercise 1.15) The president of a large software development company has become concerned about competitors learning proprietary information. He has determined to stop them. Part of his security mechanism is to require all employees to report any contact with employees of the company's competitors, even if it is purely social. Do you believe this will have the desired effect? Why or why not?

2. (*20 points*; handout, exercise 2.4) Consider a computer system with the set of rights { *r*, *w*, *x*, *a*, *l*, *m*, *o* }.
   a. Using the syntax in class (and in section 2.3 of the handouts), write a command **delete_all_rights**(*p*, *q*, *s*). This command has *p* delete all rights the subject *q* has over an object *s*.
   b. Modify your command so that the deletion can occur only if *p* has *m* rights over *s*.
   c. Modify your command so that the deletion can occur only if *p* has *m* rights over *s* and *q* does *not* have *o* rights over *s*.

3. (*30 points*; handout, exercise 2.6) This question asks you to consider the consequences of not applying the principle of attenuation to a computer system.
   a. What are the consequences of not applying it at all? In particular, what is the maximal set of rights subjects within the system can acquire (possibly with the cooperation of other subjects)?
   b. Suppose attenuation of privilege only applied to access rights such as *read* and *write*, but not to rights such as *own* or *grant_rights*. Would this ameliorate the situation discussed in the previous part? Why or why not?
   c. Consider a restricted form of attenuation, which works as follows. Associated with each subject *p* is an ancestor right a_p. A subject *q* is attenuated by the maximal set of rights that it, or any subject to which *q* has ancestor rights. So, for example, if any ancestor of *q* has *r* permission over a file *f*, *q* can also *r f*. How does this affect the spread of rights throughout the access control matrix of the system?

4. (*40 points*; handout, exercise 3.1) Prove or give a counterexample:
   The predicate can•share(*a*, **x**, **y**, G_0) is true if and only if there is an edge from **x** to **y** in G_0 labelled *a*, or if the following hold simultaneously:

i. there is a vertex **y** in G_0 with an **s**–to–**y** edge labelled *a*;
ii. there is a subject vertex **x**′ such that **x**′ = **x** or **x**′ initially spans to **x**;
iii. there is a subject vertex **s**′ such that **s**′ = **s** or **s**′ terminally spans to **s**; and
iv. there is a sequence of subjects **s**′ = $\mathbf{x}_1$, …, $\mathbf{x}_n$ = **x**′ with $\mathbf{x}_i$ and $\mathbf{x}_{i+1}$ ($1 \leqslant i < n$) being connected by an edge labelled *t*, an edge labelled *g*, or a bridge.

Send email to bishop@cs.ucdavis.edu.

Department of Computer Science
University of California at Davis
Davis, CA 95616–8562

Page last modified on 4/11/2000