

## Homework 2

**Due Date:** April 19, 2001

**Points:** 100

1. (20 points; text, exercise 1.3) The aphorism “security through obscurity” says that hiding information provides some level of security. Please give an example of a situation in which hiding information does not add appreciably to the security of a system. Give an example when it does.
2. (20 points; text, exercise 2.5) Let  $c$  be a copy flag and let a computer system have the set of rights  $\{ r, w, x, a, l, m, o \}$ .
  - a. Using the syntax in class (and in section 2.3 of the text), 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 only those rights with an associated copy flag are copied. The new copy should *not* have the copy flag.
3. (40 points; text, exercise 3.1) 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  $G_0$  labelled  $\alpha$ , or if the following hold simultaneously:
  - a. there is a vertex  $\mathbf{s} \in G_0$  with an  $\mathbf{s}$ -to- $\mathbf{y}$  edge labelled  $\alpha$ ;
  - 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  $\mathbf{s}$ ; and
  - d. there is a sequence of subjects  $\mathbf{x}' = \mathbf{x}_1, \dots, \mathbf{x}_n = \mathbf{s}'$  with  $\mathbf{x}_i$  and  $\mathbf{x}_{i+1}$  ( $1 \leq i < n$ ) being connected by an edge labelled  $t$ , an edge labelled  $g$ , or a bridge.
4. (20 points; text, exercise 4.5) Classify each of the following as examples of mandatory, discretionary, or originator controlled policies, or a combination. Please justify your answers.
  - a. The file access control mechanisms of the UNIX operating system.
  - b. A system in which no memorandum can be distributed without the author’s consent.
  - c. A facility in which only generals can enter a particular room.
  - d. A university’s registrar office, in which faculty can see grades of a particular student provided that student has given written permission.