IS2150/TEL2810 Introduction to Security

Homework 4

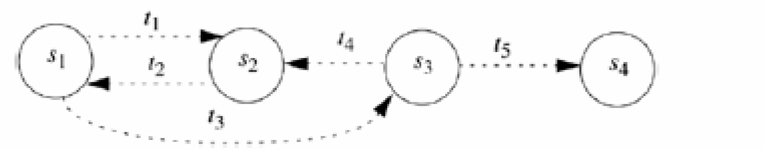
Total Points: 50
Due Date: October 5, 2007

1) From Section 4.8 Do exercise 1, 5 [15 Points]

Exercise 4.8 #1:

In Figure 4-1, suppose that edge t_3 went from s_1 to s_4. Would the resulting system be secure?

Figure 4-1. A simple finite-state machine. In this example, the authorized states are s_1 and s_2.



If the edge went from s1 to s4, then the system would be insecure because s_4 is considered part of the unauthorized states, (UA = {s3, s4}). If the edge from s_1 to s_4 were to exist, then the system would enter an unauthorized state from an authorized state.
(adapted from Annie Howard)

Exercise 4.8 #5:

Classify each of the following as an example of a mandatory, discretionary, or originator controlled policy, or a combination thereof. Justify your answers.

1. The file access control mechanisms of the UNIX operating system
   discretionary access control
   Since users can assign and modify permissions that they possess, access control is discretionary.
   (adapted from Tzu-Wei Lin)

2. A system in which no memorandum can be distributed without the author's consent
   originator access control
   This would be originator access control. This is because if I am the author of the memorandum I am the one who can say my information can be distributed, no one else can.
   (Matthew Wood)

3. A military facility in which only generals can enter a particular room
   mandatory access control
   The system controls access and an individual cannot change that. There is a somewhat tricky scenario though that could possibly make this discretionary; if there is an owner of the 'military facility' and this person also had the ability to promote military personnel to 'general'. In this way the facility owner could grant access to their facility.
   (Patrick Miller)

4. A university registrar's office, in which a faculty member can see the grades of a particular student provided that the student has given written permission for the faculty member to see them.
   discretionary access control

Here the student grants the permission to the faculty to see the grades. If he doesn't grant permission to a particular faculty member, that faculty member can't see the grades.
(Uzma Iqbal)

(Alternative)
This is a combination of an originator controlled access control policy and a discretionary access control policy. The originator, which is the registrar, controls dissemination of the data, but the student also has some control, and allows access to the individual record based upon the identity of the faculty member.

2) From Section 5.5 Do exercise 1, 2 [15 Points]

1. Why is it meaningless to have compartments at the UNCLASSIFIED level (such as (UNCLASSIFIED, { NUC }) and (UNCLASSIFIED, { EUR }))?

   There are no reasons to have compartments, or categories, because of the fact that it is unclassified, everyone can have access to it.

2. Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, both, or neither) is allowed in each of the following situations. Assume that discretionary access controls allow anyone access unless otherwise specified.

   Simple security property says that a subject can write to object if subject compartment dominates object compartment. *-property says that subject can write to object if object compartment dominates subject compartment. Let (L,C) and (L', C') be compartments for different entities. ((L,C) *dominates* $(L',C') \Leftrightarrow L' \leq L$ and $C' \subseteq C)$ is the principle we are going to apply to specify what type of access that the following sentences have.

   a. Paul, cleared for (TOP SECRET, { A, C }), wants to access a document classified (SECRET, { B, C }).
   Paul **cannot read** and **cannot write** to the document because Paul does not dominate document and also, document does not dominate Paul.

   b. Anna, cleared for (CONFIDENTIAL, { C }), wants to access a document classified (CONFIDENTIAL, {B }).
   Anna **cannot read** and **cannot write** to the document because Anna does not dominate document and also, document does not dominate Anna.

   c. Jesse, cleared for (SECRET, { C }), wants to access a document classified (CONFIDENTIAL, { C }).
   Jesse **can read** document because Jesse dominates document, but Jesse **cannot write** to the document because document does not dominate Jesse.

   d. Sammi, cleared for (TOP SECRET, { A, C }), wants to access a document classified (CONFIDENTIAL, {A }).
   Sammi **can read** document because Sammi dominates document, but Sammi **cannot write** to the document because document does not dominate Jesse.

   e. Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, { B }).
   Robin **cannot read** document because Jesse does not dominate document, but Robin **can write** to the document because document dominates Jesse.

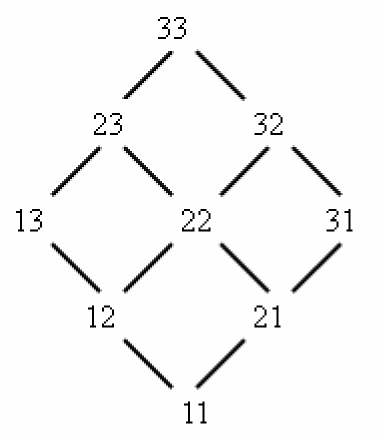
(adapted from Aref Al-Kamel)

3) Exercise on Lattice [20 Points]

Consider set of digits $D = \{1, 2, 3\}$. Let S be set of all numbers containing two digits from D; i.e., each element $a \in S$ can be written as $a = a_1a_2$ where a_1, $a_2 \in D$ (i.e., they are elements of D). For instance $a = a_1a_2 = 12$ is an element of S, as $a_1 = 1$ and $a_2 = 2$. Let relation ≈ be the "*dominance*" relation on S. For every $a, b \in S$ we say a is *dominated* by b (written as $a \approx b$) if and only if $a_1 \leq b_1$ and $a_2 \leq b_2$. (here ≤ is the "*less than or equal to*" relation on natural numbers 1, 2, and 3, i.e., $1 \leq 2$, $2\leq3$, $1\leq1$, etc.)

1. Does relation ≈ generate a *partial order* or a *total order* on the elements of *D*? Draw the *Hasse* diagram for the order it generates.

It is **partial order** because given any two numbers a, b ∈ S and not all them have relation order, such 23 and 32, which are not related to each other.



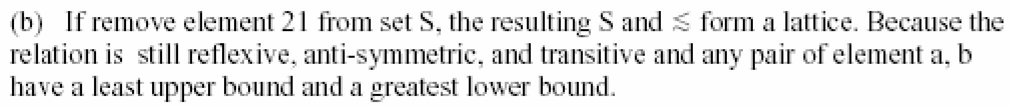
(Kuo-Hao Li)

2. Answer the following and justify it.

a. Does S and ≈ form a lattice?

R is **reflective** (a≈a for all a in S)
R is **antisymmetric** (if a≈b and b≈a, then a=b for all a,b in S)
R is **transitive**. (example: 21≈31 and 31≈32, and 21≈32)
For every s, t in S there exists a **lowest upper bound** and **greatest lower bound**.
Therefore, the relation R forms a lattice over S.
(adapted from Patrick Miller)

b. Now remove elements 21 and 22 from set S, i.e. Does the resulting set and ≈ form a lattice?



(b) If remove element 21 from set S, the resulting S and ≤ form a lattice. Because the relation is still reflexive, anti-symmetric, and transitive and any pair of element a, b have a least upper bound and a greatest lower bound.

(Uzma Iqbal)