IS-2150/TEL-2810 Introduction to Computer Security Midterm, Tuesday, Oct 12, 2005

Name:

Email:

Total Time : 2:30 Hours
Total Score : 100

There are total of 12 questions. Note that scores for each question may be different – *so spend time accordingly on each question*. Be precise and clear in your answers

---

Score

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12

Part 1

1. Mathematical foundation **[5+5]**

   1. Give the logical expression for the following statement

      a. *Not all birds can fly*

   Answer:

      b. *Every directory contains some files*

   Answer:

   2. Prove by induction the following

$$\boldsymbol{M(n)}\textbf{:}\ 1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

   Answer:

2. Write T for *true* and F for *false* for the following statements: **[10]**

[ ] Security usually is based on assumptions specific to the type of environment.

[ ] Information flow problem occurs only when unauthorized access is allowed.

[ ] One of the organizational problems in security is the question of who is responsible for the security of the computers.

[ ] In some systems (like Unix), if a subject *s* is owner of object *o*, then even if *s* has no *read* or *write* right over *o*, *s* may give *read* or *write* right over *o* to another subject. This, however, does not violate the principle of *attenuation of privilege*.

[ ] One way to prove that a given problem is *undecidable* is to reduce it to the Turing machine's halting problem.

[ ] In originator controlled access control, the owner of a file has no control over who may access the file.

[ ] In a mandatory access control model, a system mechanism controls access to an object and an individual user can occasionally alter that access.

[ ] Assume than any intrusion to a system eventually transitions the system state to an *insecure* state. If you install an *intrusion prevention* mechanism which ensures that only *known intrusions* to the system are blocked, the intrusion prevention mechanism is *precise*.

[ ] The Clark-Wilson's model shows that commercial firms do not classify data/information using multilevel scheme.

[ ] Clark Wilson model requires separation of duty feature to maintain integrity of transactions.

3. Let *a* and *b* be subjects, *z* a subject or object, and *r* be right. Write the following two acces control commands that capture the *take* and *grant* rules of the Take-Grant model. Assume that an access control matrix *A* contains the rights specified in a Take-Grant graph. The commands are specified as follows: **[5]**

   a. command *take_right*(*x*, *y*, *z*, *r*): *x* takes right *r* over *z* from *y*, provided *x* has *take* right over *y*, and *y* has *r* right over *z*.

Answer:

```
command transfer_right(x, y, z, r)
    if



end
```

b. command *grant_right*(*x*, *y*, *z*, *r*): *y* grants right *r* over *z* to *y* (provided *x* has *grant* right over *y*, and *x* has *r* right over z)

Answer:

```
command grant_right(x, y, z, r)



end
```

4. A process may send a message to another process provided that the recipient is willing to accept messages. The following class and methods are relevant: **[5]**

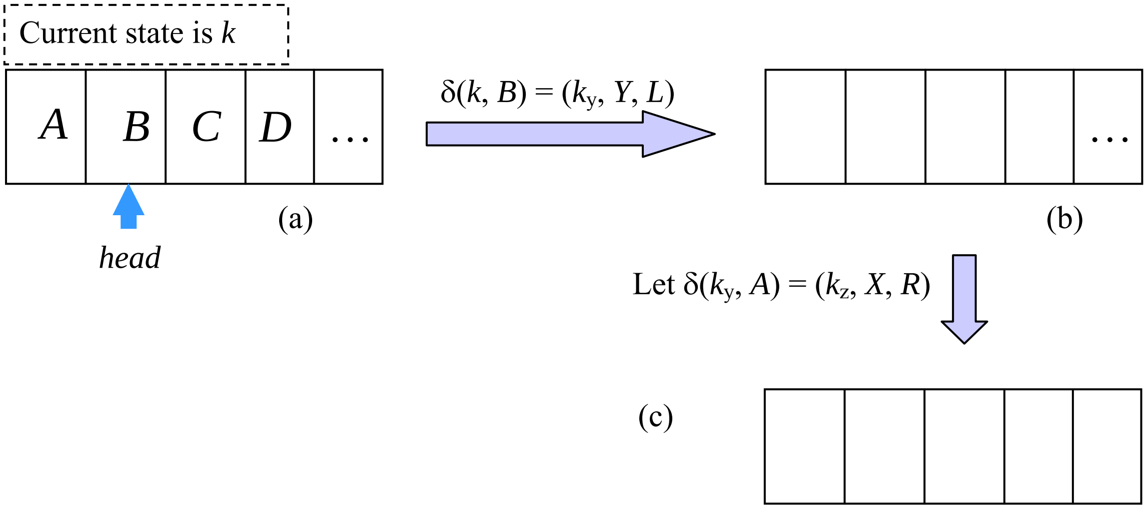
   ```
   Class Message {
       Public deposit(int processed, String message);
       Public int willaccept (int processed)
       ….
   }
   ```

   The method willaccept returns 1 if the named process will accept messages, and 0 otherwise. Write a constraint for this policy using Pandey and Hashii policy constraint language:

   Answer:

HRU Model [10]

5. Fill in the tape in (a) and (b) with the appropriate symbols based on the initial tape configuration, and the two transitions defined for the following Turing machine. Also indicate the current states and where the tape head points to after the transition.


Current state is *k*
A
B
C
D
…
head
(a)
$\delta(k, B) = (k_y, Y, L)$
…
(b)
Let $\delta(k_y, A) = (k_z, X, R)$
(c)

Fill the (i) tape entries and show the head position; and (ii) enter the rights in the three access control matrices below that correspond to the diagrams (a), (b) and (c):

Answer:

For (a)

	S_1	S_2	S_3	S_4
S_1				
S_2				
S_3				
S_4				

For (b)

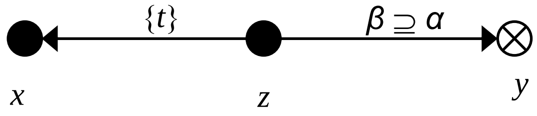
	S_1	S_2	S_3	S_4
S_1				
S_2				
S_3				
S_4				

For (c)

	S_1	S_2	S_3	S_4
S_1				
S_2				
S_3				
S_4				

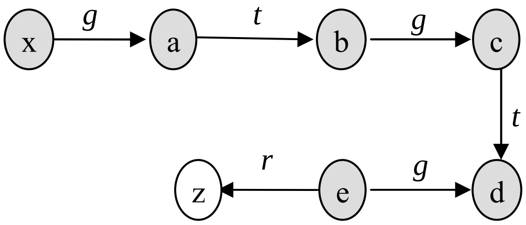
Take-Grant Model [5 + 10]

6. For the following show a *witness* such that *can_share*(α, ***x***, ***y***,*G*0) becomes true (i.e., there is a path labeled α from *x* to *y* in the final graph. Show the graphs after application of each rule in the witness.



Answer:

7. For the following Take-grant graph, show the conspiracy graph. Draw the conspiracy graph and state which subjects are involved in a conspiracy resulting in *x* gaining right *r* over z.



Answer:

(draw the conspiracy graph here)

Access Sets

A\{x\} =
A\{a\} =
A\{b\} =
A\{c\} =
A\{d\} =
A\{e\} =

Deletion set

δ(x, a) =
δ(a, b) =
δ(a, c) =
δ(b, c) =
δ(c, d) =
δ(c, e) =

8. Consider the following modifications to the owner-based policy in examples in section 3.4.1 as follows:
    - There is an object type called *file*; and there are two different types of subjects, say *user*$_1$ and *user*$_2$
    - An owner can pass only rights over an object it owns to another subject of the same type.

    Formulate this owner-based policy using SPM. Let RC = Ø, RI = {*r:c, w:c, a:c, x:c*}

Answer:

9. Specify the take grant model using SPM. Let the subject type be `subject` and object type be `object`. Fill up the following

Answer:

```
TS =
TO =

RC =
RI =

For all subjects p and q

   link(p, q)=
   f(subject, subject) =

can-create and create rules

   cr(subject, subject) =
   cr(subject, object)  =


   cc =
```

Confidentiality Policy [10]

10. Consider levels S = Secret, and T = Top-secret, and compartments X and Y. A security level is the tuple (l, c) where $l \in \{S, T\}$ and $c \subseteq \{X, Y\}$. Following is the definition of the *dominates* relation:

   The security level (l, c) *dominates the security level* (l', c') *if and only if the following hold*:

   i. $l' \leq l$

   ii. $c' \subseteq c$

   a. Draw the lattice generated by this definition for the given levels (i.e., S and T) and the compartments (i.e., X and Y). Note that you have to have elements of type (S, $\{X, Y\}$) not just category sets. [4]

   Answer:

   b. Consider the following pairs of security levels for answering the two questions that follow.

   [3, 3]

   i. (S, $\{X\}$) and (T, {Y})

   ii. (S, $\{X\}$) and (T, $\{X, Y\}$)

   iii. (S, $\{X, Y\}$) and (T, $\{X\}$)

   1) For each pair, indicate if the *dominates* relation holds and show which one dominates. If the *dominates* relation does not hold, write *incompatible*.

   Answer:

   i.

   ii.

   iii.

2) For each pair, provide the *greatest lower bound* (*glb*) and the *lowest upper bound* (*lub*).

Answer:

i.

ii.

iii.

Integrity Policies [5 + 15]

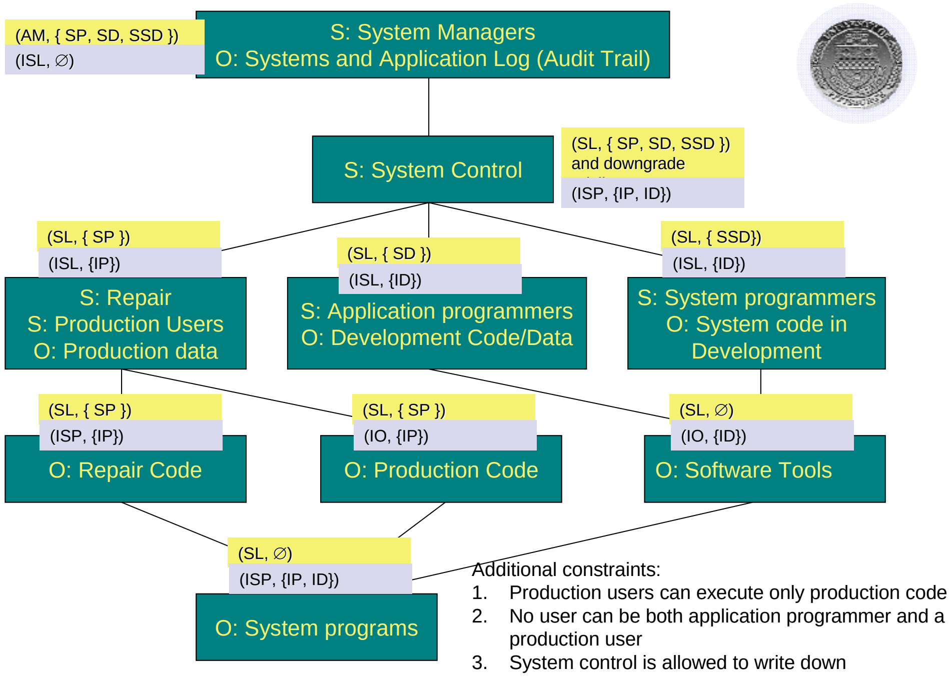
11. In the Low-water-mark policy, the following read-rule is applied:

If $s \in S$ and $o \in O$ then $i'(s) = min(i(s), i(o))$, where $i'(s)$ is the subject's integrity level after the read.

What is the idea behind this rule?

Answer:

12. Consider the diagram that specifies the security integrity levels of different entities used by Lipner. Note that these were used to address the five requirements. State, how the security level and integrity level assignment address the five requirements.



(AM, { SP, SD, SSD })
(ISL, ∅)
S: System Managers
O: Systems and Application Log (Audit Trail)

S: System Control
(SL, { SP, SD, SSD }) and downgrade
(ISP, {IP, ID})

(SL, { SP })
(ISL, {IP})
S: Repair
S: Production Users
O: Production data

(SL, { SD })
(ISL, {ID})
S: Application programmers
O: Development Code/Data

(SL, { SSD})
(ISL, {ID})
S: System programmers
O: System code in Development

(SL, { SP })
(ISP, {IP})
O: Repair Code

(SL, { SP })
(IO, {IP})
O: Production Code

(SL, ∅)
(IO, {ID})
O: Software Tools

(SL, ∅)
(ISP, {IP, ID})
O: System programs

Additional constraints:
1. Production users can execute only production code
2. No user can be both application programmer and a production user
3. System control is allowed to write down

IS2150/TEL2810: Introduction to Computer Security 17

Answer:

I. *Users will not write their own programs, but will use existing production programs and databases.*

II. *Programmers will develop and test programs on a nonproduction system; if they need access to actual data, they will be given production data via a special process, but will use it on their development system.*

III. *A special process must be followed to install a program from the development system onto the production system.*

IV. *The special process in requirement 3 must be controlled and audited.*

V. *The managers and auditors must have access to both the system state and the system logs that are generated.*