IS2935 Introduction to Computer Security
Midterm,
Thursday, Oct 21, 2004

Name:

Email:

Total Time : 2:30 Hours
Total Score : 100

The questions have been grouped into four parts. These parts roughly correspond to the different sets of chapters/topics indicated.

Part 1:	Total Score 20
Part 2:	Total Score 30
Part 3:	Total Score 25
Part 4:	Total Score 25

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

A separate sheet has been provided that contains definitions that may be useful in answering the questions.

Score

Questions	Part 1	Part 2	Part 3	Part 4
Total				
Total =				

Best of Lucks!!

(*Read the questions carefully***)**

Part 1

1. Define/explain the following terms: **[2]**

   Accountability

   Non-repudiation

2. Write T for *true* and F for *false* for the following statements: **[8]**

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

   [ ] Disruption refers to unauthorized interruption of correct operation of a function.

   [ ] Covert channels makes the information flow problem more difficult to solve.

   [ ] 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 violates the principle of *attenuation of privilege*.

   [ ] One way to prove that the general *safety* problem is *undecidable* is to reduce the safety problem 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*.

3. Let *x* and *y* be subjects, *z* a subject or object, and *r* be right. Write the following acces control command that captures the *grant* rule 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: **[4]**

a. 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*)

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

end

4. Consider the following class and methods: **[6]**

```
Class File{
    Public file(String name);
    Public String getFilename();        // returns the name of the file
    Public day invalidDay;
    Public boolean beingWritten;
    Public char read();
    ….
}
```

The meanings of methods and variables are as follows

- invalidDay indicates the day on which the access to the file is to be denied. For example, if "invalidDay == Moday," it means that the associated file cannot be allowed to be read.
- beingWritten is a Boolean variable that is either TRUE or FALSE. If it is TRUE then it indicates that the file is being written into (or modified) by someone. If it is FALSE then it means the file is not being written into (or modified).

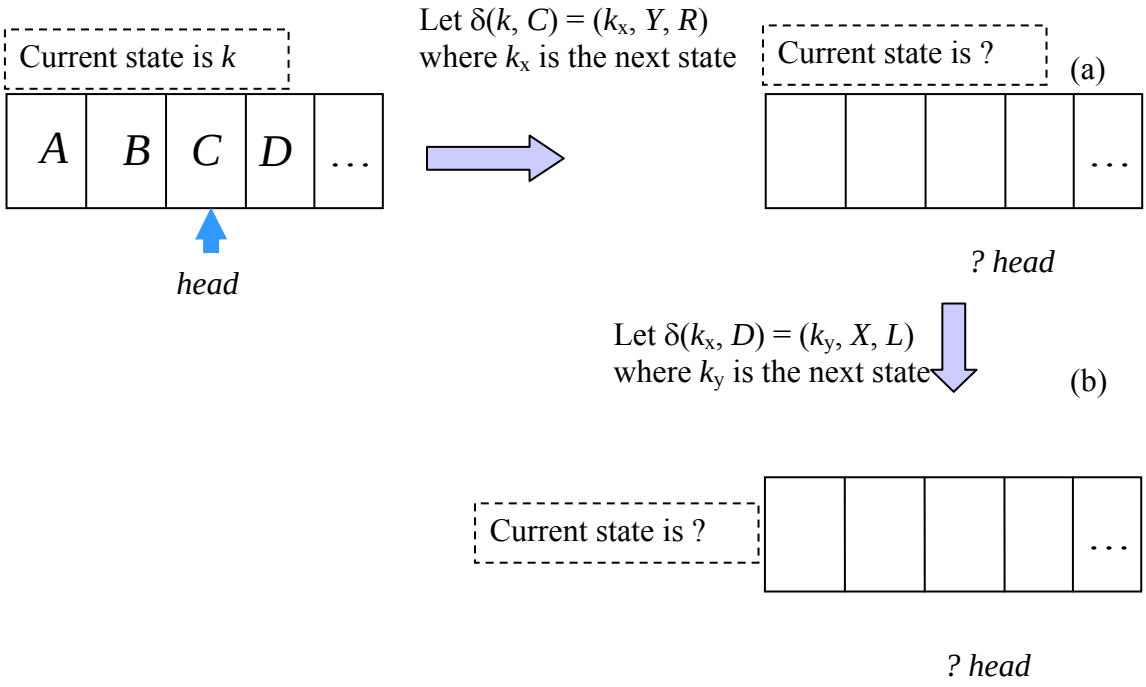
Assume that variable Date.currentDay indicates the current day, i.e, if "Date.currentDay == Tuesday," it indicates that the current day is Tuesday. Write the following policy using Pandey and Hashii policy constraint language:

A downloaded program can read a file on the system only if (a) the file is not currently being written into (no modification is in progress), and (b) the day of access is valid.

Part 2

HRU Model [10]

1. Consider the Turing Machine figure shown and do the following:
   a. 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.

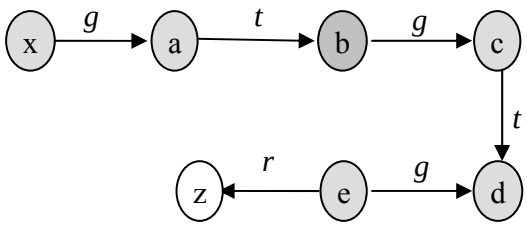


   b. If we assume that this Turing machine maps to the safety problem of the HRU access control matrix model, give the set of generic rights that we know from the diagram:

Answer:

Take-Grant Model [10]

2. 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*. Show the witness.



(draw the conspiracy graph here)

Access Sets

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

Deletion set

$\delta(x, a)$ =
$\delta(a, b)$ =
$\delta(a, c)$ =
$\delta(b, c)$ =
$\delta(c, d)$ =
$\delta(c, e)$ =

Witness

Schematic Protection Model [10]

3. Consider the following owner-based policy:
    a. There are three subject types st_1, st_2, and st_3, and three object types ot_1, ot_2, ot_3 such that $st_3 < st_2 < st_1$ and $ot_3 < ot_2 < ot_1$, (similar to dominates relations among security levels)
    b. A subject of type st_i can only *create* an object of type ot_i,
    c. A subject of type st_i can only give the *read* rights that it has over an object of type ot_i to another subject st_j if an only if $st_i \leq st_j$,
    d. A subject of type st_i can only give the *write* rights that it has over an object of type ot_i to another subject st_j such that $st_j \leq st_i$,

Consider the following sets of rights $RI = \{r{:}c, w{:}c\}$, $RC = \varnothing$. For the above policy, define the required *link*, *filter*, *can-create* (*cc*) and *create-rule* (*cr*) functions that implement the above policy.

Answer:

Part 3

1. Write T for *true* and F for *false* for the following statements: **[5]**

   [ ] If $(RS, n) = (\{r1, r2, r3\}, 2)$ defines a SSD constraint, then the user assignment UA = {(u, r1), (u, r2)} is not valid.

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

   [ ] Lipner's model using only the Bell_LaPadula scheme (security levels) was found to be too flexible to control and hence, it was augmented with Biba's integrity levels.

   [ ] The confidentiality policy $c(i_1, i_2, ..., i_n) = (i_1, i_3, i_7)$, where $n > 7$, indicates that a security mechanism envorcing this policy may reveal information only about inputs i_1, i_3, and i_7.

   [ ] If the confidentiality policy is specified as $c(i_1, i_2, ..., i_n) = (i_1, i_3, i_7)$, where $n > 7$, it means that the information related to i_1, i_3, i_7 should should be leaked out by a mechanism.

Confidentiality Policy [10]

2. Consider *sensitivity levels* S = Secret, and T = Top-secret, and *compartments* A and B. A security level is the tuple (l, c) where $l \in \{S, T\}$ and $c \subseteq \{A, B\}$. 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 complete lattice of security levels generated by the given sensitivity levels and (i.e., S and T) and the compartments (i.e., A and B).

   Answer:

b. Consider the following pairs of security levels for answering the two questions that follow.
   i. $(S, \{A, B\})$ and $(T, \{B\})$
   ii. $(S, \{A\})$ and $(T, \{A, B\})$
   iii. $(S, \{A, B\})$ and $(T, \varnothing)$

   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, [10]

3. In the *Low-water-mark* policy, the following read-rule is applied: **[5]**

   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?

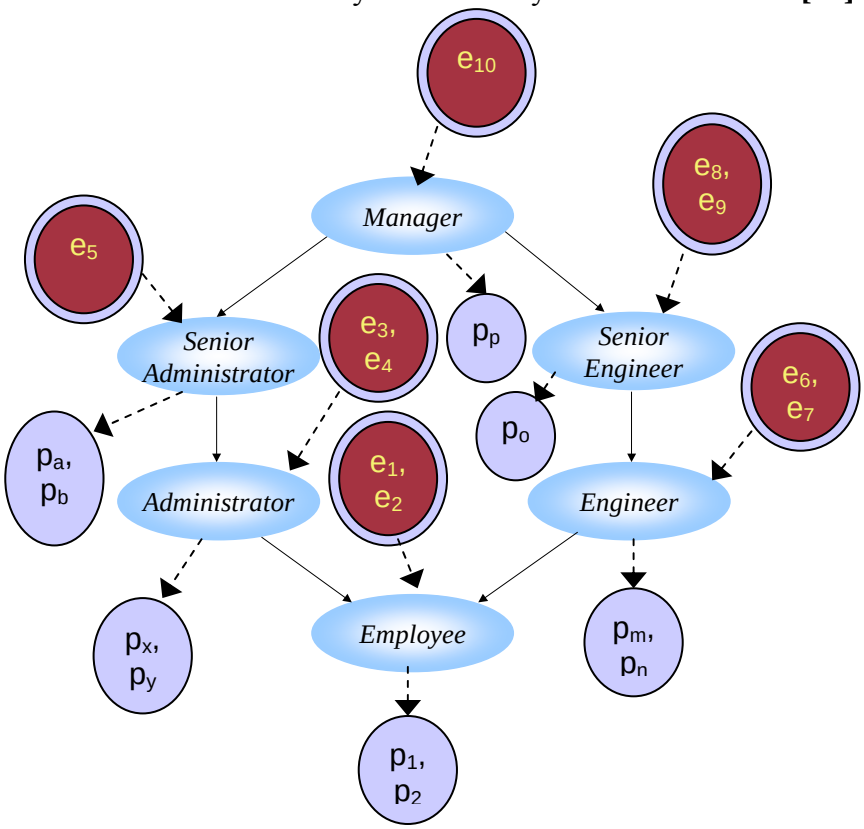
   Answer:

1. Assume that Alice and Bob are friends. Consider two conflict of class sets COI_1 = {X, Y} and COI_2 = {U, V}. Let CD_X, CD_Y, CD_U, and CD_V be the company data sets of companies X, Y, U and V. Illustrate using these, what kind of assignments are prohibited by the Chinese wall policy. **[5]**
   (***Provide your answer at the back of a question page***)

Part 4

RBAC, Multiple policies, Design Principles [25]

2. In the figure below p_i's represent permissions and e_i's represent users. Their assignments to roles in the hierarchy are shown by the dotted arrows. **[10]**



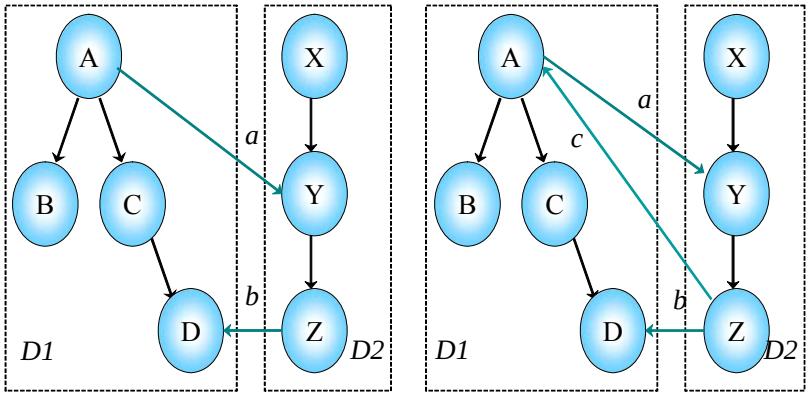
i. Let $(\{r_1, r_2, r_3, r_4\}, 3) \in SSD$, which of the following UA sets are valid:

- $UA_1 = \{(u_1, r_1), (u_2, r_1), (u_3, r_1), (u_1, r_2), (u_4, r_2), (u_5, r_2), (u_1, r_3), (u_2, r_3), (u_3, r_3), (u_4, r_4)\}$
- $UA_2 = \{(u_1, r_1), (u_3, r_1), (u_5, r_1), (u_1, r_2), (u_2, r_2), (u_3, r_2), (u_5, r_2), (u_2, r_3), (u_4, r_3), (u_4, r_3)\}$

Provide reasons for your answer.

ii. Differentiate between SSD and DSD. Suppose we have $(\{r_1, r_2, r_3, r_4\}, 3) \in SSD$ and $(\{r_1, r_2, r_3, r_4\}, 3) \in DSD$ – what are the implications of having both of these separation of duty constraints present in a system at the same time.

4. Consider two domains D1 and D2 as shown in the figures (*i*) and (*ii*). F_{12} indicates the permitted access between the two domains in each case. In the figure, assume that the arrow from a node to another indicates that the subject representing the first node has access to all objects that the subject that represents the latter node can access. For (*i*) and (*ii*), indicates whether there is a violation of *principle of security* or a *principle of authority*. If there is a violation of one of the principles, give possible solutions. **[5]**



F_{12} = {a, b}

(*i*)

F_{12} = {a, b, c}

(*ii*)

Answer:

1. Write what the following design principles mean. **[10]**

Fail-safe defaults

Open design

Economy of mechanism

Psychological acceptability

Complete mediation