IS-2150/TEL-2810 Introduction to Computer Security Midterm, Thursday, Oct 12, 2006

Name:

Email:

Total Time : 2:30 Hours
Total Score : 100

There are total of 10 questions. Note that scores for each question is 10, although the time required for each may vary – *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

Good Luck **!**

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

[y] In DG/UX, the virus protection region can be considered as at a higher integrity level than the integrity level of the user region..

[ ] The `umask` value prevents any user from making illegal permission assignments using `chmod` command.

[ ] Confidentiality policies address the issue of how to control information flow.

[ ] Biba's low water mark integrity model is exact dual of the Bell-Lapdula model

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

[ ] The command
`chmod 5754 hello.txt` is the same as
`chmod u+srwx g+rx o+r hello.txt".`

[ ] In BellLapadula model, the read *right* includes the *execute* right.

[ ] One advantage of role based access control model is that it can be used to enforce diverse set of policies including Biba and Bell-Lapadula models.

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

[ ] To enforce Chinese-Wall policy, a system must be capable of maintaining access histories of each user..

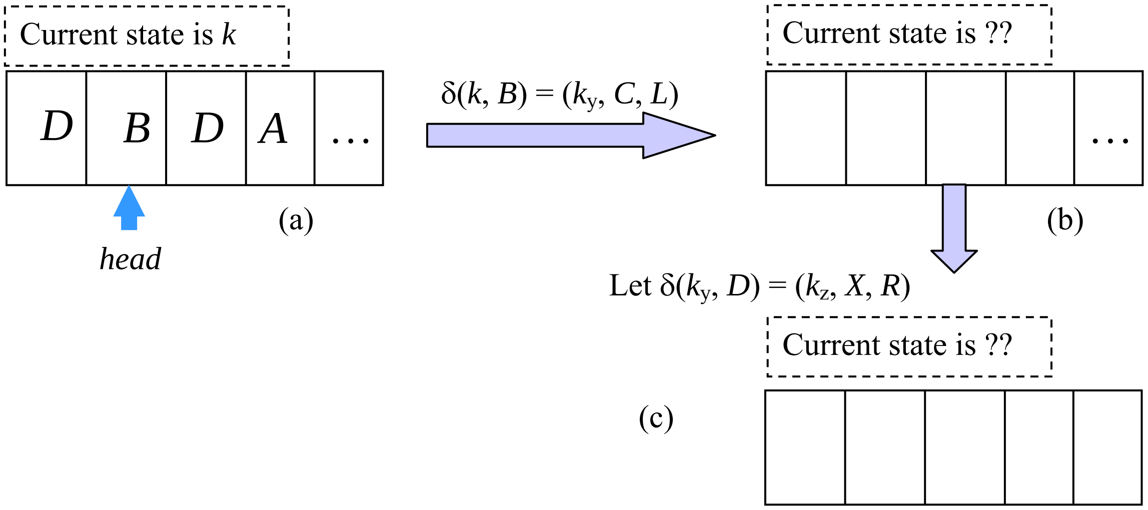
2. Do the following **[Score 10]**
    a. Let the set of rights be {*read, write, execute, modify*}. Write the command *delete_all_rights*(*p, q, s*) that causes *p* to delete all the rights that subject *q* has over *s*, if the following condition holds - *p* has *modify* rights over *s* and *q* does *not* have own rights over *s*. Checking for absence of right is not allowed.
    b. Note that in a command if there are multiple conditions, they are joined by AND operation (i.e., in (a)). Why is the use of OR operation to combine two conditions unnecessary?
    (*provide answer on the backside of the adjacent page*)

3. Briefly describe Shirley’s four classes of threats and then map the following attacks to these four threat classes. **[Score 10]**
    - Interruption, delay, denial of receipt or denial of service
    - Interception or snooping
    - Modification or alteration
    - Fabrication, masquerade, or spoofing
    - Repudiation of origin

4. Describe the *setuid* bit related problem in Unix systems. What does *read*, *write* and *execute* permissions mean for Unix directories. **[Score 10]**

5. Discuss how the Clark-Wilson model stands in terms of Lipner’s five requirements? **[Score 10]** ***(provide answer on the backside of the adjacent page)***

6. 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. **[Score 10]**



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				

7. 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: **[Score 10]**

   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.

   Answer:

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

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

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

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

   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.

8. Assume two *Conflict of Interest* classes COI_1 and COI_2. Let CD_X_1, CD_X_2 and CD_X_3 be the datasets of COI_1 (here, X_1, X_2, $X,_3$ are companies). Similarly, let CD_Y_1, CD_Y_2 and CD_Y_3 be the company datasets in COI_2. Assume that you have a consultancy firm with a number of consultants employed. When providing consultancy services assume that it may involve *read*, *write* or both accesses to the company dataset. Let the following be the requirements:

   Providing consulting services to X_1 requires *read* and *write* access to CD_X_1.
   Providing consulting services to X_2 requires *read* access to CD_X_2.
   Providing consulting services to X_3 requires *read* and *write* access to CD_X_3.
   Providing consulting services to Y_1 requires *read* and *write* access to CD_Y_1.
   Providing consulting services to Y_2 requires *read* access to CD_Y_2.
   Providing consulting services to Y_3 requires *read* access to CD_Y_3.

   What is the *minimum* number of consultants you would need to ensure that you provide consultancy services to the six companies as per the Chinese Wall model? Show the consultant to company assignments. **[Score 10]**

   Answer:

9. Let the following be the role hierarchy relationships, $RH = \{(r_1, r_2), (r_1, r_3), (r_2, r_4), (r_2, r_5), (r_3, r_5), (r_3, r_8), (r_6, r_3), (r_6, r_7), (r_7, r_8)\}$. Note that (r_i, r_j) means r_i is senior of r_j. Let each role be *assigned* to exactly one user. We can assume that u_i is *assigned* to role r_i. Further, note that if u is assigned to r that means u is authorized for r. Based on these, answer the following. **[Score 10]**

- Find *authorized_users*(r_5) and *authorized_users*(r_8)?
- Assume you want to include a static separation of duty (SSoD) constraint ($\{r_2, r_3, r_4, r_7$), 3). What problem arises by the introduction of this SSoD into the system? How would you change the SSoD so that it is satisfied by the existing RH and the user assignments?

Answer:

10. What does the following terms mean? Briefly explain. **[Score 10]**
(consider only FIVE of them)

Social Engineering

Broad security mechanism

Tranquility

Separation of function

Dynamic Separation of Duty in RBAC model

Originator Controlled Access Control