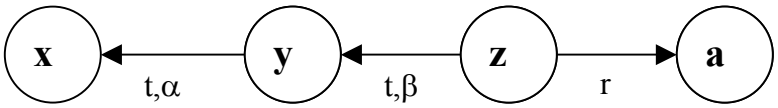
# School of Information Technology
# IIT Kharagpur

**Course Id: IT60112 Information and System Security** **Mid Sem Exam**
**Date: February 22, 2007** **Total Time: 2 Hours**
**Max. Marks: 60**

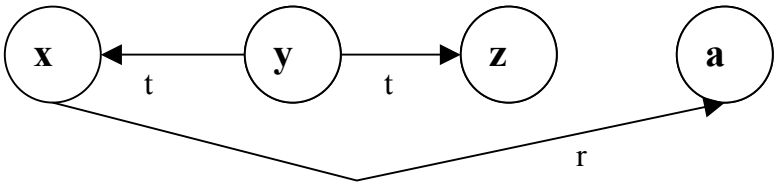
*Instructions: Answer all questions. You may answer the questions in any order. However, all parts of the same question must be answered together. Clearly state any reasonable assumption you make.*

1. Consider the following pair of initial and final graphs representing protection states of a system where each node represents a subject. t and g stand for take and grant rights while α, β and r are arbitrary rights.

Initial




Final




Is there a valid sequence of graph rewriting rules to achieve the final state from the initial state? If yes, draw each intermediate graph, clearly identifying the rule that was applied at each step. If no, clearly explain why it cannot be achieved. **[10]**

2. Consider a database system in which access control is enforced through evaluation of Boolean expressions. The various users, their groups and roles are as follows:

| **user** | **group** | **role** |
|---|---|---|
| Amit | Programmer | Team Member |
| Kaushik | Analyst, Designer | Team Leader, Manager |
| Nitin | Programmer, Analyst, Designer | Team Member |

The database tables have the following default access rules

| **Mode of Access** | **Default Rule** |
|---|---|
| Select | 1 |
| Insert | 0 |
| Delete | 0 |
| Update | 1 |

Specific rules for access to the tables Employee, Accounts, Project and Design are given below.

| Table | Rules |
|---|---|
| Employee | Select: 'Analyst' in subject.group or 'Team Member' in subject.role; Delete:1 |
| Accounts | Insert:0; Update: 'Manager' in subject.role and 'Programmer' in subject.group |
| Project | Select:1; Delete:1; Insert:0; Update: time.hour <14 and time.hour > 10 |
| Design | Select:0 |

(a) Draw the access control matrix for the above protection system at 11:00 AM.
(b) If the default access rules table is changed so that default rule for all the four modes of access (i.e., Select, Insert, Update and Delete) is 0, draw the new access control matrix of the protection system at 7:00 PM. **[5+5=10]**

3. Consider the set of generic rights G = {read, write, own} and a Command ADD_RW_RIGHTS (a, b, c) in the HRU model. This command causes subject **a** to give write and read rights to **b** on **c** only if **a** owns **c**.
   (a) Write the interpretation of this command in terms of the primitive operations as defined in the HRU model.
   (b) Starting with an arbitrary protection state before the execution of the command, show the final protection state at the end of execution of the command. You must also show the intermediate states at the end of each primitive operation.
   (c) Let us state the Principle of Attenuation of Privileges (POAP) as follows: "A subject can only give a right it possesses while executing any primitive operation." Consider that ADD_RW_RIGHTS (a, b, c) you have defined above must also satisfy the POAP. In that case, is the following protection state transition valid? If yes, write the new interpretation of ADD_RW_RIGHTS (a, b, c) augmented with POAP. If no, clearly and precisely state why no. **[5+5+5=15]**

| | P1 | P2 | O1 |
|---|---|---|---|
| P1 | | | own |
| P2 | | | |

to

| | P1 | P2 | O1 |
|---|---|---|---|
| P1 | | | |
| P2 | | | write, read |

4.
   (a) Why is Bell LaPadula model called a Lattice model of security?
   (b) What is the difference between certifications and enforcements in the Clark-Wilson's Integrity policy?
   (c) State the requirements of a commercial system as suggested by Lipner.
   (d) Explain how Clark Wilson's Integrity policy handles the Principle of Separation of Duty and Auditing requirements. **[5+3+4+3=15]**

5. Consider a password-based authentication system in which all passwords are of length between 8 to 10 characters chosen from an alphabet of size 20. To prevent Dictionary Attack of Type 2, it employs a backoff strategy such that it takes 1 sec. to try the first password and subsequent backoff periods form an Arithmetic Progression series of common diff. 2 sec. After 5 failed attempts, it disconnects. The periods of disconnections form a series of duration 1 second, 2 seconds, 4 seconds, 8 seconds, etc. The backoff series is not reset after disconnection. That is, if the attacker reconnects and tries, the backoff time will continue the original series.

   A Dictionary Attack of Type 1 can be launched on the authentication system in which the rate of checking of passwords is 50 per second. How many passwords can be tried using Type 2 attack during the same time in which the probability of finding a password using Type 1 attack is 0.8? Consider all passwords to be equally likely. **[10]**