School of Information Technology
IIT Kharagpur

Course Id: IT60112 Information and System Security (End-semester Examination)

Date: April 23, 2012 **Total Time: 3 Hours**
Max. Marks: 100

Instructions: Answer any four 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. For the following questions, zero or more options may be correct. Each correct answer carries 2.5 marks. 1 mark will be deducted for every wrong answer. An answer will be considered correct if all the correct and only the correct choices have been selected. If you are not attempting a question, write "Not answered". If you feel none of the options is correct, write "None". **[2.5×10=25]**

(i) In Take Grant Protection model
   a. Safety is undecidable
   b. Take and grant rules can only be invoked (i.e. initiated) by subject nodes
   c. Rights granted by one subject to another subject cannot be revoked (i.e., removed)
   d. Rights granted by one subject to another object cannot be revoked (i.e., removed)

(ii) In Kerberos (Ver. 4) with two realms A and B, a secret key is shared between
   a. The authentication server of A and the authentication server of B
   b. The authentication server of A and the ticket granting server of B
   c. The ticket granting server of A and the ticket granting server of B
   d. The ticket granting server of A and each application server of B

(iii) S/Key one time password based authentication system does NOT support the following secure system design principle(s)
   a. Principle of least privilege
   b. Principle of psychological acceptability
   c. Principle of open design
   d. Principle of complete mediation

(iv) In HRU model, the following do(es) NOT vary from one system to another
   a. The set of primitive operations
   b. The set of commands
   c. The set of generic rights
   d. The definition of leakage of right

(v) If an information transfer path exists between object o_1 to object o_{n+1},
   a. Biba's Low Water Mark policy enforces that $i(o_1) >= i(o_{n+1})$
   b. Biba's Ring policy enforces that $i(o_1) \neq i(o_{n+1})$
   c. Biba's Strict Integrity policy (Biba's Model) enforces that $i(o_1) < i(o_{n+1})$
   d. Biba's Ring policy enforces that $i(o_1) > i(o_{n+1})$

(vi) In Role Based Access Control (RBAC)
   a. User to role assignment (UA) is a relation defined on U×R
   b. Permission to role assignment (PA) is a relation defined on P×R
   c. Role Hierarchy (RH) is a relation defined on R×R
   d. Only one user is associated with each session

(vii) Misuse based intrusion detection systems usually have
- a. Low values of false positive
- b. High values of false positive
- c. Low values of true negative
- d. High values of true negative

(viii) Role mining
- a. is a bottom-up approach to role engineering
- b. is a top-down approach to role engineering
- c. always has a unique solution for a given UPA matrix
- d. decomposes a given UPA matrix into UA and PA matrices

(ix) TCSEC
- a. specified both functional and assurance requirements
- b. was primarily meant for evaluation of secure operating systems
- c. is the current international standard for evaluating security of systems
- d. suffered from the problem of "criteria creep"

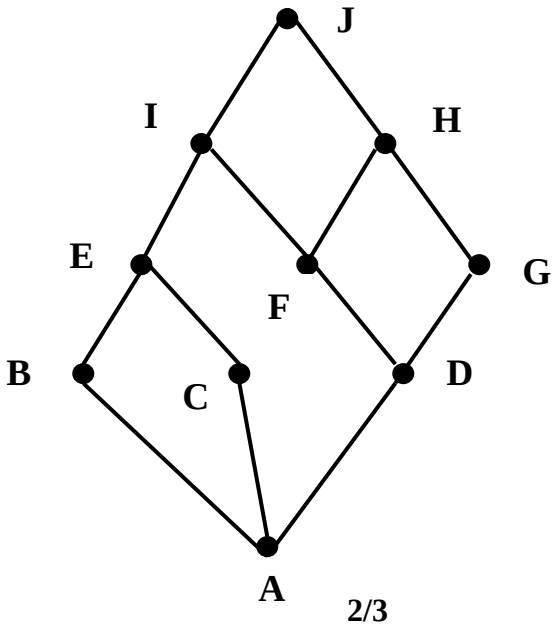
(x) TRBAC
- a. is used to specify RBAC policies in which roles can be enabled or disabled based on time
- b. supports role triggers
- c. represents time with the help of periodic expressions
- d. is used to specify RBAC policies in which roles can be enabled or disabled based on the location of the user

2.

(a) Write a periodic expression to represent an infinite set of time intervals such that each interval begins at 9:00 am of every Monday, Tuesday and Wednesday of every week of the months of January, March, June and October of every year and lasts for 2 hours.

(b) Consider a set of prioritized event expressions S = {H:enable R0, H:disable R0, VH:enable R1, H:disable R1, L:enable R1, H:enable R2, VH:disable R2}. Determine the set of all members of S that are not blocked by S, i.e., determine the set Nonblocked(S). Assume the priority order as VH>H>L.

(c) Consider the following role hierarchy in an RBAC system. Modify the role hierarchy by creating private sub-hierarchy(ies) so that a subset of the permissions of roles D, F, G and H are not inherited by J. Also mention to which of the roles, users can be assigned in the new hierarchy. **[10+7+[6+2]=25]**



3. Consider the following UPA relation in an access control system implementing RBAC:

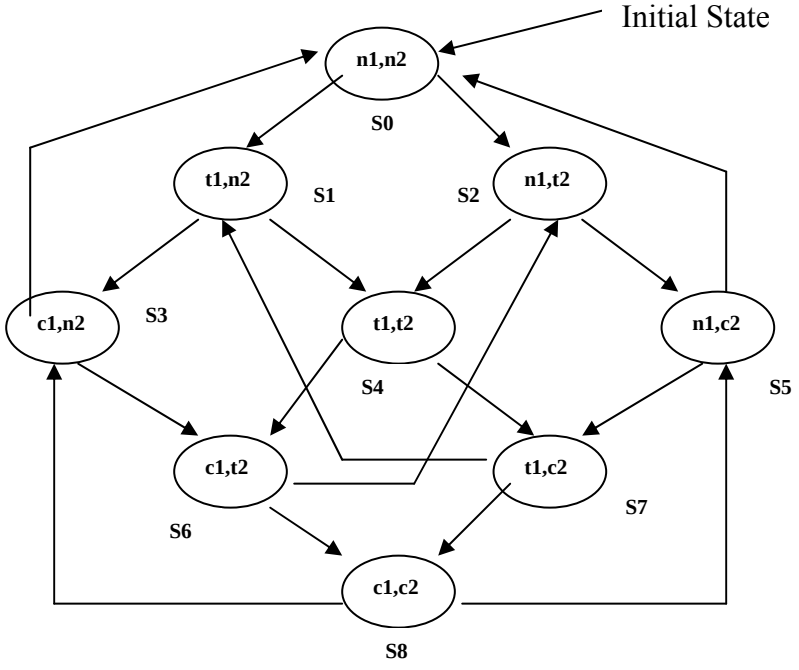
UPA = { (u1,p1), (u1,p2), (u1,p4), (u1,p5), (u2,p2), (u2,p3), (u3,p2), (u3,p3), (u3,p5), (u3,p6), (u4,p1), (u4,p2), (u4,p4), (u4,p5), (u4, p6) }

(a) Construct a bipartite graph from the above relation.
(b) Draw a biclique cover for this graph with at most 7 bicliques. From this biclique cover, write the UA and PA relations. If such a solution cannot be obtained, write "Impossible to generate".
(c) Consider a Boolean matrix representation of the UPA relation given above with users as rows and permissions as columns. Make a decomposition of this matrix into two matrices A and B where rows and columns of A represent users and roles, respectively, and rows and columns of B represent roles and permissions respectively. The number of columns of A should be 3 and the decomposition is δ-consistent with the original matrix for a δ value of 8. If such a solution cannot be obtained, write "Impossible to generate".

[3+[8+4]+10=25]

4. Consider the following model of a system that was meant to enforce mutual exclusion. *P1* and *P2* are two processes. For *i=1&2*, *ni* denotes not in critical section, *ti* denotes trying to enter critical section and *ci* denotes currently in critical section for process *Pi*.

(a) Using CTL specify one safety property, one non-blocking property and one liveness property that should be satisfied by a system designed for enforcing mutual exclusion.
(b) For the given model, state with justification which of the properties mentioned by you in (a) above are satisfied and which are not.
(c) State a fourth property you would like to specify for the system (it could be a hypothetical property, i.e., need not necessarily be a true safety, non-blocking or liveness property) in English language as well as in CTL. State with justification whether the model satisfies the property or not. **[6+12+[4+3]=25]**



5. Briefly explain the following concepts with example(s) wherever appropriate **[6.25×4=25]**

(a) Role Hierarchy in RBAC
(b) Different types of constraints in RBAC
(c) Dictionary attacks on a password based authentication system
(d) Peer review for assurance