School of Information Technology
IIT Kharagpur

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

Date: April 29, 2011 **Total Time: 3 Hours**
Max. Marks: 100

Instructions: Answer any 4 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 two anomaly based intrusion detection systems (IDSs) A and B. IDS A raises alarm 95% of the time there is intrusion. If there is no intrusion, it does not raise an alarm 95% of the time. IDS B raises alarm 90% of the time there is intrusion. If there is no intrusion, it does not raise an alarm 99% of the time. Let us denote the probability of occurrence of no intrusion when an alarm is raised to be K. (a) What should be the rate of occurrence of intrusion in the system being protected (in units of number of intrusions per 1000 instances) so that one of the IDSs has twice the value of K as compared to the other? (b) If the rate of occurrence of intrusion obtained above is doubled, what will be the new ratio of the values of K for IDSs A and B? Interpret your answer. **[15+10=25]**

2. 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. You need to only write the option(s). If none of the options is valid, write "None". **[2.5 x 10=25]**
   (i) In Kerberos (Ver. 4), a client has to contact the Authentication Server
      a. Once for each session
      b. Twice for each session
      c. Once for each application server
      d. Once for each service request
   (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. Each application server of A with each application server of B
   (iii) In Kerberos (Ver. 4), session key is shared between
      a. A client and the authentication server
      b. The authentication server and the ticket granting server
      c. A client and the ticket granting server
      d. A client and each application server that it accesses
   (iv) In Kerberos (Ver. 4), authenticators help to
      a. Prove the identity of the client to the ticket granting server
      b. Prove the identity of the ticket granting server to the authentication server
      c. Prove the identity of the client to the application server
      d. Establish reverse authentication between the ticket granting server and the client
   (v) In Biba's Low Water mark policy
      a. Any subject can write to any object
      b. Any subject can read any object
      c. Any object can read any object
      d. Any object can execute any object at a lower integrity level

(vi) In Chinese Wall Security Policy implementing both simple security condition and *-property

a. The least number of distinct subjects is the same as the number of Conflict of Interest classes
b. The maximum number of distinct subjects is the same as the number of Company Datasets
c. The maximum number of distinct subjects is the same as the number of Conflict of Interest classes
d. The least number of distinct subjects is the same as the number of Company Datasets

(vii) In HRU model

a. The set of primitive operations is fixed (i.e., does not vary from one system to another)
b. The set of generic rights is fixed (i.e., does not vary from one system to another)
c. The set of commands is fixed (i.e., does not vary from one system to another)
d. The set of constraints is fixed (i.e., does not vary from one system to another)

(viii) The S/Keys onetime password based authentication system uses the principle of

a. Least privilege
b. Psychological acceptability
c. Open design
d. Failsafe default

(ix) TCSEC

a. was primarily used for evaluating operating systems
b. defined both functional requirements as well as assurance requirements
c. used to take longer for evaluation as compared to ITSEC
d. was a standard developed in Europe

(x) In the context of role mining:

a. δ-approx RMP is likely to generate the same or higher number of roles as the value of δ is increased.
b. When the role mining problem is mapped to the database tiling problem, each tile represents a role
c. When the role mining problem is mapped to the minimum biclique cover problem, each biclique represents a session
d. Min-noise RMP problem minimizes the number of roles for a given number of permissions

3. Explain the following concepts with examples wherever appropriate

(a) TCSEC
(b) Configuration management
(c) Peer Review
(d) Misuse based and Anomaly based intrusion detection
(e) Role mining using minimum bilclique cover finding **[5x5=25]**

4.

(a) Briefly explain the various components of RBAC0, RBAC1, RBAC2 and RBAC3 along with the functions to mathematically represent the user of a session, roles available in a session and permissions available in a session
(b) Describe how RBAC1 can be implemented as RBAC2.
(c) Consider the ERP system of the institute that you use. Suggest how its access control can be designed using RBAC model (for roles like Faculty, HOD, Dean, etc., whose details you might not know directly, suggest a set of permissions that you feel appropriate). You have to describe appropriate content of the sets U, R, P, relations UA and PA as well as possible hierarchies and constraints.

(d) Suppose we want to extend the access control policies of the above system using TRBAC. Specify a representative Role Enabling Base for the new system that includes 5 periodic events and 3 role triggers. Each periodic event should be clearly specified first in English language and then formally using time interval, periodic expression and prioritized event expression. Role triggers also should be specified first in English language and then represented formally using simple event expressions, role status expressions, prioritized event expression, delay expression, etc. **[8+3+6+8=25]**

5. Consider the following model of a system to enforce mutual exclusion. P1 and P2 are two processes. For i 1 and 2, Non-critical state is denoted by ni, trying to enter critical section is denoted by state ti and currently in critical section is denoted by state ci.

(a) Using CTL, specify one safety property, one liveness property and one non-blocking property that you deem appropriate for such a system designed for enforcing mutual exclusion.
(b) Show which of these properties are satisfied and which are not for the model. You must clearly explain why you feel they are satisfied or give a counter-example to show that they are not.
(c) State a fourth property you would like to specify for the system (it could be a hypothetical property and need not really be truly a safety, liveness or property) and write it in English language as well as in CTL. Show whether the model satisfies the property or not. You must clearly explain why you feel it is satisfied or give a counter-example to show that it is not. **[6+12+7=25]**