School of Information Technology
Indian Institute of Technology, Kharagpur

IT60112 Information and System Security **Mid Semester Examination**
Date: February 22nd, 2005. **Total Time: 2 Hours** **Max. Marks: 80**

Answer All Questions. Clearly write any reasonable assumption that you make.

Q1. IIT Kharagpur defines a security policy that lets the use of e-mails on a particular system to only faculty and staff. Students cannot send or receive mails on that host. Classify the following mechanisms as secure, precise or broad. Give reasons for your answer.

(a) E-mail sending and receiving programs are disabled.
(b) For every e-mail being sent or received, the system checks in a database to see if the party is a valid faculty or staff. If so, the mail is processed, else rejected.
(c) The e-mail sending program asks the user if he or she is a student. If so, the mail is refused. The e-mail receiving programs are disabled.

[2X3=6]

Q2.
(a) Define a formal model of a Protection System in terms of its various components.
(b) Consider the set of generic rights {*read, write, execute, append, list, modify, own*} in the context of a protection system.
    (i) Using primitive operations and constraints, define a command DELETE_ALL_RIGHTS (p,q,s) which causes subject p to delete all rights that the subject q has over an object s.
    (ii) Modify your command in (i) so that the deletion can occur only if p has *modify* rights over s.
    (iii) Modify your command so that the deletion can occur only if p has *modify* rights over s and q does not have *own* rights over s.
    (iv) Using the primitive operations, write a command COPY_ALL_RIGHTS (p,q,s) that copies all rights that p has over s to q.
    (v) Modify your command in (iv) so that only those rights with an associated copy flag are copied. The new copy should not have the copy flag.

[5+(3X5)=20]

Q3.
(a) Formally define a Program, a Security Policy for the program and a Protection Mechanism for the program.
(b) Let M1 and M2 be two protection mechanisms for a program Q under a given security policy I. Prove that
    (i) M1 $\cup$ M2 is as precise as M2 $\cup$ M1 with respect to Q under I
    (ii) If M1 and M2 are themselves secure, then M1 $\cup$ M2 is also secure for Q under I

[5+(6X2)=17]

Q4. Define and give one example each of the following:

(a) Identity based access control
(b) Rule based access control
(c) Originator controlled access control

[3X3=9]

Q5. Given the security levels Top Secret (TS), Secret (S), Confidential (C) and Unclassified (U) (ordered from highest to lowest) and categories A, B and C, specify which types of access (read, write, append, execute) will be allowed for the following subjects and objects under Bell-LaPadula Model

(a) Ram (TS, {A,C}) ←→ firstfile (S,{B,C})
(b) Sita (C, {C}) ← → secondfile (C, {B})
(c) Atul (S, {C}) ← → thirdfile (C, {C})
(d) Anil (TS, {A,C}) ← → fourthfile (C, {A})
(e) Dhiren with no clearance (and hence, works at the unclassified level) ← → fifthfile (C, {B})

[2X5=10]

Q6.

(a) State the five security requirements of a commercial system as suggested by Lipner.
(b) Explain how Separation of Duty is incorporated in Lipner's model. Construct an Access Control Matrix for Lipner's commercial model. The matrix will have entries for r(read), w(write) and a(append) rights.
(c) Show that the matrix is consistent with the five requirements you have stated.

[5+5+2=12]

Q7.

(a) Define an Information Transfer Path
(b) State Biba's Strict Integrity Policy
(c) Prove that if there is an Information Transfer Path from object $o_1 \in O$ to object $o_{n+1} \in O$, then enforcement of the Strict Integrity Policy requires that $i(o_{n+1}) \leq i(o_1)$ for all $n > 1$ where O is the set of objects.

[2+2+2=6]