SASTRA DEEMED UNIVERSITY

(A University under section 3 of the UGC Act, 1956)

End Semester Examinations

May 2025

Course Code: **INT313**

Course: **COMPUTER SYSTEM SECURITY**

QP No. **:U096-6**

Duration: **3** hours

Max. Marks**:100**

PART - A

Answer all the questions **10 x 2 = 20 Marks**

1. Discuss whether the following is a violation of Confidentiality, Integrity or Availability.
   a) Eavesdropping data packets sent in the Local area Network
   b) Modifying the Password file in the Computer System.
   c) Sending excessing traffic into local area network
   d) Altering the entries of the records in Domain Name servers.
2. Define Computer system security using security of states and transitions.
3. What is an Integrity Policy? Give an example of an integrity Policy?
4. Discuss the standard concerned with the use of Trusted Systems.
5. State the Unwinding theorem for non-interference security in Computer systems.
6. Which Security Policy considers the history of past accesses to datasets?
7. What are the two types of covert channels found in computer systems?
8. What are Sandboxes? Give an example from Computer System usage.
9. What are the various types of Security Policies used in organizations?

10. What are the threats that require digital forensics investigation?

PART - B

Answer any Four questions **4 x 15 = 60 Marks**

11. a) Consider the following commands for an Access Control Matrix. Show the resulting access control matrix after executing all the commands:
Create subject UserA; Create subject User B; Create File1; Create Program1; enter read for [userA,File1]; Enter execute for [UserB, Program1]; enter write for [UserB, File1]; enter execute for [userA, Program1]. Enter own for [UserA, File1]; Enter own for [UserB,Program1]
Create the Access Control Lists for File1 and Program1. Create the capability lists for User A and User B. (8)

b) Discuss Discretionary Access Control Model, Mandatory Access Control Model and Role Based Access Control Model with examples. (7)

12. a) Discuss the Bell Lapadula Model's Simple Security Property and *-property using Security Labels and Categories Discuss the Bibas integrity Model using Security Labels and categories. (8)

b) Discuss how the Lipner's Integrity Matrix model combines the Bell Lapadula Model and Biba Models. (7)

13. The security of a computer System can be modelled using states and transitions. Consider a two-bit machine where two bits representing the HIGH and LOW bit. The system can be in any of the four states (0,0), (0,1), (1,0) and (1,1). Users issue commands to the system and the commands are executed in the order they are given. Users observe the outputs based on the certain privileges. For example, user A can see the output of both bits while the user B sees only the LOW bit. Define noninterference Secure property based on the outputs observed by the users for the above system when the commands issued are xor0 and xor1 by userA and userB. Consider the system where commands issued by User A affect only the HIGH bit and the commands issued by User B affect only the LOW bit. Is this system non-interference secure?

14. a) Discuss how information flows in the following Programming Language statements: x=y+z; (8)
(i) The statement $x=y+10$;
(ii) If $x = 1$, then $y=0$; else $y= 1$;
(iii) If $x=1$ then $y=a$; else $y=b$;
(iv) $x=y+z$

b) Discuss how covert channels may be created by observing the following activities in the Computer System. (i) By observing the average CPU utilization after a specified time period (ii) By observing the presence or absence of a file in a directory. (7)

15. a) Specify how the root user of a Unix System can protect data and processes from other users when both system programs and user programs are being run in the computer system.

b) Create a policy for User Authentication into the Computer System administered by the root user.

c) The root user has to ensure that the users comply with the permissions given to them for accessing files on the secondary storage. What procedure can be implemented to check users comply with the permissions given to them?

d) How can we ensure that user programs do not access files on the secondary storage if permissions are not given?

16. Consider the Confidentiality and Integrity of database Tables in a Relational DataBase systems. The DBMS manages tables and relationship between the tables on behalf of the user.
a) Discuss the authentication and authorization procedure for accessing the records in a table of a DBMS.

b) Assume the administrator wants to enforce confidentiality and integrity checks to some columns in a table. Discuss the procedure for enforcing this policy.

c) Discuss how we can infer violations of confidentiality and Integrity policies on the records of the DBMS.

d) Discuss how the auditing function can work for the above database management system.

PART – C

Answer the following **1 x 20 = 20 Marks**

17. Develop a Security Policy for an organization involved in software Development. There are various users who are developers, System administrators, installers and auditors. There are various types of workstations used for tasks such as Development, Production. The programmers cannot access the production systems and data. The software programs must be installed in the production system using a special procedure which is done only by the installers. The auditors monitor the installation procedure. The auditors will be given permission to read the files in the developers workstations as well as the production workstations. The System administrators only have access to the production system. Your task is create a multilevel policy with confidentiality and integrity constraints.

a) Create Security Labels for allowing read access to developer programs and data and production programs and data.

b) Create Security Labels for allowing write access to developer programs and data and production programs and data.

c) Assign Security clearances for reading and writing to developer programs and data and production programs and data.

d) Assign Security clearance for installing programs into the production system.

e) Verify all the confidentiality and Integrity requirements specified in the above description.

***