**Birla Institute of Technology & Science, Pilani**

**Work Integrated Learning Programmes Division**

**First Semester 2022-2023**

**Mid-Semester Test**

**(EC-2 Regular)**

Course No. : SS ZG681

Course Title : Cyber Security

Nature of Exam : Open Book

Weightage : 30%

No. of Pages = 3

No. of Questions = 5

Duration : 2 Hours

Date of Exam : 25/09/2022 (Evening)

Note to Students:

1. Please follow all the *Instructions to Candidates* given on the cover page of the answer book.
2. All parts of a question should be answered consecutively. Each answer should start from a fresh page.
3. Assumptions made if any, should be stated clearly at the beginning of your answer.
4. Consider you have the responsibility of IT security in a university. Universities maintain Student Information System (SIS), a web-based platform that helps colleges and departments maintain student data online for easier management and access. The system is used to collect and store university-wide student data so that teachers, students, and administrators can easily access it. Student Information System is also called with different names such as Student Management System (SMS), Student Information Management System (SIMS), or Student Records System (SRS). Student data that is collected includes student information such as their name, address, phone number, and email id; student grades; student records of tests; student attendance; and student’s certifications and voluntary contributions. For students’ access the university provides students a university student number (USN), and a card, which contains a PIN, for account access.

Only from the information given in the problem statement, identify at least three examples of assets and for each of these assets assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively in case a security breach were to occur. Justify your answers. [2 x 3 = 6]

1. Consider a data facility shown in figure consisting of a piece of land enclosed with a high fence. Inside the fence, there is a communications closet and data (tapes, disks, microfilms, etc.) storage shed. In the communications closet, network cables pass. If an adversary wants to steal data, two approaches exist. Stealing a backup tape or disk or the attacker can put a probe on the network cable in the communications closet and perform traffic analysis. Draw a simple attack tree describing possible ways to accomplish the goal. [8]



As discussed in the class, show leaf nodes representing different ways to initiate an attack. Indicate sub-nodes (you may choose them to be AND-nodes or OR-nodes or a combination of both). Note that to achieve the goal represented by an AND-node, all the subgoals represented by that node’s subnodes must be achieved. To achieve the goal represented by an OR-node, at least one of the subgoals must be achieved.

1. Suppose there are four security levels (ordered from highest to lowest): Top Secret (TS), Secret (S), Confidential (C) and Unclassified (U) and categories Math, Biology, and Chemistry. Indicate which types of access (read, write, append, execute) will be allowed for the following subjects and objects under Bell-LaPadula Model. Justify your answer. Assume that discretionary access is given. [6 x 1 = 6]

(a) Mani (TS, {Math, Chemistry, Physics}) ← → file\_A (S,{Physics, Chemistry})

(b) Nanda (C, { Chemistry }) ← → file\_B (C, { Physics })

(c) Faiz (C, { Chemistry }) ← → file\_C (C, {Chemistry })

(d) Saisha (C, { Physics }) ← → file\_D (S, {Chemistry, Physics })

(e) Pranjal (TS, {Math, Chemistry }) ← → file\_E (C, {Math})

(f) Rituraj with no clearance (and hence, works at the unclassified level) ← → file\_F (C, { Physics })

1. Suppose you apply for a job for a suitable position in a company, go through the interview process and finally are selected. You join the organization; go through the necessary orientation and training programs before being allocated to projects. For performing your job, if you need access to any resource, your organization’s policy expects you to make requests for getting access to specific resources. Every time you need access to a resource, you need to make an explicit request. What type of security design principle your organization is following? Describe this design principle. Clearly explain the design principle with examples. What happens if this kind of design principle is not followed?

Consider you are a Security Architect in your organization. A complex system has more changes of having security problems. In addition, too complex the system is, too many opportunities for something to go wrong. You would like to create small reusable components for repeated functionality. Which design principle is applicable in this scenario? Describe the design principle. Clearly explain the design principle with an example. [1 + 1 + 2 + 1 = 5]

1. How can organizations identify vulnerabilities in their system?

Explain briefly the differences between vulnerability, threat, exploit, and risk.

Explain a situation with an example where there is no risk even when there is a vulnerability.

[1 + 2 + 2 = 5]

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*