National University

Of Computer & Emerging Sciences Faisalabad-Chiniot Campus

Name: **Section:** **Roll:**

Information Security
Quiz 01

Q1: What are the three main methods of malware detection? Briefly explain each method.

Three Main Methods of Malware Detection

Signature Detection
Matches known malware patterns; only detects existing viruses.

Change Detection
Uses file integrity checks (e.g., hashes) to spot unexpected changes.

Anomaly Detection
Defines normal system behavior; flags deviations as suspicious.

For more information refer to **Lecture 03 Slide 25**

Q2: In each of the following scenarios, **identify which security design principle is being followed or violated**. Clearly justify your answer.

A. The company behind Telegram messenger hired some brilliant cryptographers to design proprietary security protocols for secret chats.

Open Design Violated

Keeping the protocol secret makes security rely on obscurity rather than public review, so this breaks the open-design principle.

B. Staff at an airline booking office are required to provide their password as well as scan their smart card before confirming a booking.

Separation of Privilege Followed

Requiring both a password and a smart-card enforces two independent checks before access is granted.

C. A program successfully opens a file in write mode, but after a few hours, writing data to file fails due to permission errors.

Complete Mediation Followed

Permissions are being re-checked (not just at open), so when they're revoked the write fails — the system mediates each access.

(Also acceptable to call this ***Least Privilege Followed*** *if you interpret the change as temporary removal of elevated rights.)*

For more information refer to **Lecture 04 Slides 4-5.**

Q3: Case Study **(Security Objectives)**

You've been hired as a cybersecurity consultant for a healthcare organization that has recently suffered a data breach. During a briefing with the executive team, they ask you to explain the fundamental concepts that should guide their information security strategy moving forward.

Explain the CIA triad in information security, and describe how each component contributes to the overall security of the organization's information system, particularly in the context of protecting patient data.

Solution:

The CIA triad refers to Confidentiality, Integrity, and Availability, the three core principles that guide information security.

- Confidentiality ensures that patient data is only accessible to authorized users. This protects sensitive health information from unauthorized disclosure or breaches.
- Integrity guarantees that patient records remain accurate and unaltered, preventing tampering or corruption of critical medical data.
- Availability ensures that healthcare staff can reliably access patient information whenever needed, which is essential for timely diagnosis and treatment.

Together, the CIA triad provides a balanced framework to secure patient data, maintain trust, and support safe healthcare operations.

For more information refer to **Lecture 01 Slides 22-34.**