9/10

National University of Computer and Emerging Sciences, Lahore Campus

Course:	Information Security	Course Code:	CS 3002
Program:	BS (DS)	Semester:	Fall 2024
Duration:	30 Minutes	Total Marks:	10
Paper Date:	02-Sept-24	Weight	
Section:	7C	Page(s):	[redacted]
		Roll. No.	
Exam:	Quiz 01	Name:	

Instruction/Note Honesty always gives fruit and Dishonesty is always harmful.

Question no 1: 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. (5 marks)

C – Confidentiality : Meaning that data is not accessible to unauthorized users.

I – Integrity : Meaning that the data is not compromised.

A – Accessibility / Availability: meaning that it available at the time of need.

→ Confidentiality: In terms of protecting patient data, confidentiality is very important because it might contain personal data about the patient (i.e Age, DOB, Address) which can be used in illegal activities.

⇒ Integrity: The integrity of the data is also very important because the data might contain information about the drugs that the patient is allergic to and if that is somehow not shown ~~or~~ altered in some way then that could have fatal consequences

→ Availability: For example the doctor has to perform surgery on a patient and he needs to find out vital information about the patient (i.e blood group or age) in an emergency situation, it is very important that the data is accessible at that time.

Question no 2: You are part of a team responsible for designing a new access control system for a government agency's database. During the planning phase, a debate arises over the security measures that should be prioritized to prevent unauthorized access, especially in the event of a system failure.

Explain the principle of "Fail-Safe Defaults" in security design to your team. Discuss why this principle is essential for maintaining system security, particularly in the context of protecting sensitive government data. (5 marks) 4

In case of a system failure, there are some settings that are pre-defined in case disaster strucks. These settings are very minimal and strict so that only certain people can access the data. In case of protecting government data that could be the president, prime minister of the chief of army. These ~~off~~ default, strict settings are called "fail-safe defaults". This is to make sure that in case someone with malicious intent crashes the system somehow, they still won't be able to access the system. If government's data is exposed then that could have catastrophic consequences. Another security measure that we can implement is enable multi-user authentication. For example if somehow the system crashes, then at least two of the senior member's approval is required to access the system again.