1. Breach of Confidentiality, Integrity and Breach of availability

Confidentiality, integrity, and availability (CIA) is a model designed to guide policies for information security within an organization. In this context, confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of ready access to the information by authorized people. The model is sometimes known as the CIA triad.

1. Confidentiality prevents sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. A good example is an account number or routing number when banking online. Data encryption is a common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication is becoming the norm and biometric verification is an option as well. In addition, users can take precautions to minimize the number of places where the information appears, and the number of times it is actually transmitted to complete a required transaction.
2. Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). In addition, some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash. If an unexpected change occurs, a backup copy must be available to restore the affected data to its correct state.
3. Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed, providing a certain measure of redundancy and failover, providing adequate communications bandwidth and preventing the occurrence of bottlenecks, implementing emergency backup power systems, keeping current with all necessary system upgrades, and guarding against malicious actions such as denial-of-service (DoS) attacks.
4. Denial of Service:

A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

1. **Theft of services** is the legal term for a crime which is committed when a person obtains valuable services — as opposed to goods — by deception, force, threat or other unlawful means, i.e., without lawfully compensating the provider for these services. It may also overlap with some types of fraud in which payment is made on credit, but under an assumed identity, and ultimately disavowed.
2. Real-time applications usually are executed on top of a Real-time Operating System (RTOS). Specific scheduling algorithms can be designed. When possible, static cyclic schedules are calculated off-line. If more flexibility is needed on-line techniques are applied. These algorithms are bound to priorities which can be assigned statically or dynamically. Designing a proper RTOS architecture needs some delicate decisions. The basic services like process management, inter-process communication, interrupt handling, or process synchronization have to be provided in an efficient manner making use of a very restricted resource budget. Various techniques like library-based approaches, monolithic kernels, microkernels, or virtual machines/exokernels are applied, based on specific demands. Safety critical application can be supported by separation of applications either in the time or the space domain. Multi-core architectures need special techniques for process management, memory management, and synchronization. The upcoming Wireless Sensor Networks (WSN) generate special demands for RTOS support leading to dedicated solutions. Another special area is given by multimedia applications. Very high data rates have to be supported under (soft) RT constraints. Based on the used encoding techniques (e.g. MPEG) dedicated solutions can be created.
3. Application of MIS to management

A **management information system** (**MIS**) provides information that organizations require to manage themselves efficiently and effectively. Management information systems are typically computer systems used for managing. The five primary components: 1.) *Hardware,* 2.) *Software,* 3.) *Data (information for decision making),* 4.) Procedures (design,development and documentation), and 5.) People (individuals, groups, or organizations). Management information systems are distinct from other information systems because they are used to analyze and facilitate strategic and operational activities.

1. Practical Answer
2. Information management is mainly concerned with people managing information sources, that is, auditing them, acquiring and storing them for easy retrieval and dissemination of information and one has to make it a point that they are well preserved. whereas knowledge management involves people in creating, capturing, sharing and using knowledge in an organisation.

**Questions:**

1. Security violations of the system can be categorized as intentional (Malicious) or accidental. Describe the following security violations and how do they affect information management?
   1. Breach of confidentiality
   2. Breach of Integrity
   3. Breach if Availability
   4. Theft if Service
   5. Denial of Service
2. To meet timing requirements, real time operating system must employ various techniques. Elaborate the different techniques to meet the timing requirements of real time operating system.
3. What is the application of MIS in management? Explain
4. Lay-out a chart on Lateral relationship “based on horizontal position in your organization workplace.
5. Compare and contrast Management Information System from Knowledge Management.