**Chap #9 *SECURITY***

Security is a measure of the system’s ability to protect data and information from unauthorized access while still providing access to people and systems that are authorized.

**Characteristics Of Security (CIA):**

1. **Confidentiality** is the property that data or services are protected from unauthorized access. For example, a hacker cannot access your income tax returns on a government computer.
2. **Integrity** is the property that data or services are not subjected to unauthorized manipulator. E.g., your grades have not been changed since your instructor assigned it.
3. **Availability**is the property that the system will be available for legitimate use. For example, a denial-of-service attack won’t prevent you from ordering book from an online bookstore.

**Other characteristics to support CIA:**

1. ***Authentication***verifies the identities of the parties to a transaction and checks if they are truly who they claim to be. For example, when you get an email purporting to come from a bank, authentication guarantees that it actually comes from the bank.
2. ***Nonrepudiation***guarantees that the sender of a message cannot later deny having sent the message, and that the recipient cannot deny having received the message. For example, you cannot deny ordering something from the Internet, or the merchant cannot disclaim getting your order.
3. ***Authorization***grants a user the privileges to perform a task. For example, an online banking system authorizes a legitimate user to access his account.

**Security General Scenario:**

One technique that is used in the security domain is threat modeling. An “attack tree,” is used by security engineers to determine possible threats. The root is a successful attack and the nodes are direct causes of that attack. An attack is an attempt to break CIA, and the leaves of attack trees would be the stimulus in the scenario. The response to the attack is to

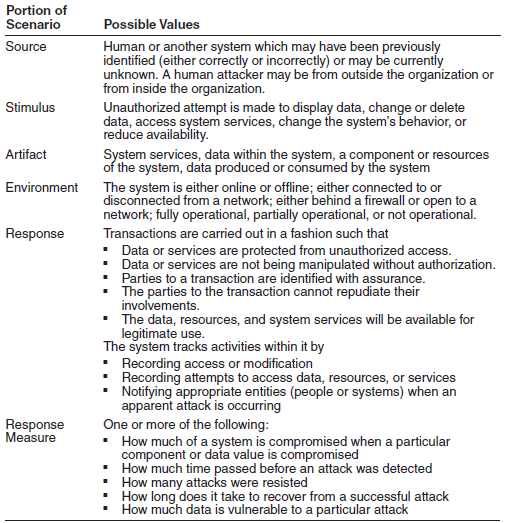
preserve. From these considerations we can now describe the security general scenario.

* **Source of stimulus:** The source of attack may be human or another system. It may be known or unknown. It may be inside or outside of the organization.
* **Stimulus:** It is an attack that may be characterized as unauthorized attempt to change or update the data.
* **Artifact:** The target of attack may be either services of data, data stored in it or data produced from it.
* ***Environment*.** The attack can come when the system is either online or offline, either connected to or disconnected from a network.
* ***Response****.* The system should ensure that transactions are carried out in a fashion such that data or services are protected from unauthorized access. The system should also track activities within it by recording access or modification notifying appropriate entities (people or systems) when an apparent attack is occurring.
* ***Measure Response****:*It include how much of a system is compromised when a particular data is compromised and after how much time how long it took to recover from a successful attack, and how much data was vulnerable to a particular attack.

these elements of the general scenario, which characterize security,

**a sample concrete scenario:** A disgruntled employee from a remote location attempts to modify the pay rate table during normal operations. The system maintains an audit trail, and the correct data is restored within a day.

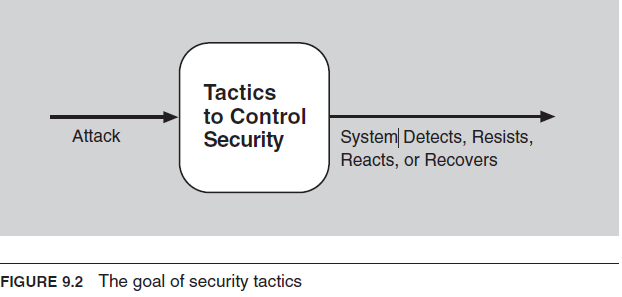
**Agr miss koi or sa sample scenaior dain tu general scenario wali headings ke hisaab se edit krlo!! Jaisa book main tariqa hai ye wala**

****

**Tactics for Security:**

One method for thinking about how to achieve security in a system is to think

about physical security. Secure installations have limited access , have means of detecting intruders have armed guards, have recovery mechanisms such as off-site backup. These lead to our four categories of tactics: detect, resist, react, and recover.

****

1. **Detect Attacks:**

The detect attacks category consists of four tactics: detect intrusion, detect service denial, verify message integrity, and detect message delay.

* **Intrusion detection:** used to monitor network traffic for suspicious activity and alerts when such activity is observed. Some IDS are capable for taking action against such malicious activity by itself.
* **Detect service denial**is the comparison of the pattern or signature of network traffic *coming into* a system to historic profiles of known denial-of service attacks.
* **Verify message integrity***.* This tactic employs techniques such as checksums or hash values to verify the integrity of messages, resource files, deployment files, and configuration files. A checksum is a validation mechanism where in the system maintains redundant information for configuration files and messages. A hash value is a unique string generated by a hashing function whose input could be configuration files or messages.
* **Detect message delay** is intended to detect potential man-in-the-middle attacks, where a malicious party is intercepting (and possibly modifying) messages. By checking the time that it takes to deliver a message, it is possible to detect suspicious timing behavior.

1. **Resist Attacks**

There are a number of well-known means of resisting an attack:

* **Identify actors.** Identifying “actors” is really about identifying the source of any external input to the system. Users are typically identified through user IDs. Other systems may be “identified” through access codes, IP addresses, protocols, ports, and so on.
* **Authenticate actors.** Authentication means ensuring that an actor (a user or a remote computer) is actually who or what it purports to be. Passwords, one-time passwords, digital certificates, and biometric identification provide a means for authentication.
* **Authorize actors.** Authorization means ensuring that an authenticated actor has the rights to access and modify either data or services. This mechanism is usually enabled by providing some access control mechanisms within a system.
* **Limit access.** Limiting access involves controlling what and who may access which parts of a system. This may include limiting access to resources such as processors, memory, and network connections, which may be achieved by using process management
* **Limit exposure.**Limiting exposure refers to ultimately and indirectly reducing the probability of a successful attack. This can be achieved by concealing facts about a system to be protected or by dividing and distributing critical resources so that the exploitation of a single weakness cannot fully compromise any resource.
* **Encrypt data.** Data should be protected from unauthorized access. Confidentiality is usually achieved by applying some form of encryption to data and to communication. Encryption provides extra protection to the data.

1. **React to Attacks**

Several tactics are intended to respond to a potential attack:

* *Revoke access.* If the system or a system administrator believes that an attack is underway, then access can be severely limited to sensitive resources, even for normally legitimate users and uses.
* *Lock computer*. Repeated failed login attempts may indicate a potential attack. Many systems limit access from a particular computer if there are repeated failed attempts to access an account from that computer. Legitimate users may make mistakes in attempting to log in. Therefore, the limited access may only be for a certain time period.
* *Inform actors*. Ongoing attacks may require action by operators, other personnel, or cooperating systems. Such personnel or systems must be notified when the system has detected an attack.

1. **Recover from Attacks**

Once a system has detected and attempted to resist an attack, it needs to recover. Part of recovery is restoration of services. For example, additional servers or net- work connections may be kept in reserve for such a purpose. Since a successful attack can be considered a kind of failure, the set of availability tactics that deal with recovering from a failure can be brought to bear for this aspect of security as well.

Question in exam:

1. General scenario OF security
2. Security tactics