INFORMATION SECURITY

Introduction

Information security

- Information security (IS) is designed to protect the confidentiality, integrity and availability of computer system data from those with malicious intentions. Confidentiality, integrity and availability are sometimes referred to as the CIA Triad of information security.

Information security

- Information security (infosec) is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information.
- Infosec responsibilities include establishing a set of business processes that will protect information assets regardless of how the information is formatted or whether it is in transit, is being processed or is at rest in storage.

Information systems

- An information system is a set of interrelated components that collect, process, store and distribute information to support decision making and control in an organization.
- Now a days, majority of computerized IS relies on data warehouse and DBMS s/w to manage the storage and retrieval of the information in the system.

Threats to information system - introduction

- Information systems security is the integrity and safety of its resources and activities.
- Threat is a possible event that can harm an information system
- Vulnerability is the degree of exposure in view of a threat
- A countermeasure is a set of actions implemented to prevent threats

- It can be distinguished as ‘information-level threats’ and ‘network-level threats’.
- Network-based threats become effective when attacker requires network access to corporate computer systems or to networks used by corporate computer systems.
- Ex – hacking of computer systems and launching of DoS attacks as well as spreading malicious, such as viruses.

- Information-level threats also make heavy use of network but at the primary level is the content of a message and not its form.
- Ex- sending fake inquiries to service accounts to eat up resources (e.g. flooding the mail server with many messages so that it gets choked).

Information systems security – threats and attacks

Security threats have four principal sources:

1. Human error:
   For example, inadvertent disclosure of confidential information.
2. Computer abuse or crime:
   Example is, when a person intends to be malicious and starts to steal information from sites, or cause damage to, a computer or computer network.

3. Natural and political disasters:
This can happen in the form of natural calamities and wars, riots, etc.

4. Failure of hardware or software:
server malfunctioning, software errors etc.

Computer crime is defined as any illegal act in which a computer is used as the primary tool. Computer abuse is unethical use of a computer. Security threats related to computer crime include:
1. Impersonation: the impersonator enjoys the privileges of a legitimate user by gaining access to a system by identifying oneself as another person after having defeated the identification and authentication controls employed by the system

2. Trojan horse method: Concealing within an authorized program a set of instructions that will cause unauthorized actions.

3. Logic bomb: Unauthorized instructions, often introduced with the Trojan horse technique, which stay dormant until a specific event occurs, at which time they bring into effect an unauthorized act

4. Computer viruses: Segments of code that are able to perform malicious acts and inserts copies of themselves into other programs in the system

5. DoS: Rendering the system unusable by legitimate users

6. Dial diddling: changing data before or during input, often to change the contents of database

7. Salami technique: Diverting small amounts of money from a large number of accounts maintained by the system. These small amounts will not be noticed.

8. Spoofing: Configuring a computer system to masquerade as another system over the network in order to gain unauthorized access to the resources the system being mimicked is entitled to.

9. Super-zapping: Using a system's program that can bypass regular system controls to perform unauthorized acts.

10. Scavenging: Unauthorized access to information by searching through the residue after a job has been run on a computer.

11. Data leakage: there are variety of methods for obtaining a data stored on the system. The data may be encoded into an innocuous report in sophisticated ways.

12. wiretapping: tapping computer TC lines to obtain information

13. Theft of mobile devices: this is a new dimension that is coming up given the increase in mobile workforce

The three pillars of information security

Confidentiality: In the domain of IS, the concept of confidentiality is used as an attempt to prevent the intentional or unintentional disclosure of message contents. Loss of confidentiality can occur in many ways, such as through the intentional release of private company information or through a misapplication of network rights.

Integrity: The concept of integrity ensures that
1. Modifications are not made to data by unauthorized personnel or processes.
2. Unauthorized modifications are not made to data by authorized personnel or processes.
3. The data are internally and externally consistent.

Availability: the concept of availability ensures the reliable and timely access to data or computing resources by the appropriate personnel. It guarantees that the systems are up and running when they are needed

Important terms

- Identification: It indicates the means by which users claim their identities to a system. It is most commonly used for access control, and is necessary for authentication and authorization
- Authentication: This is the testing of evidence of a user's ID. It establishes the user's ID and ensures that users are who they say they are. Authentication is a security measure designed to establish the validity of a transmission, message or originator, or a means of verifying an individual's eligibility to receive specific categories of information

Accountability: A system's ability to determine the actions and behavior of the single individual within a system, and to identify that particular individual

Authorization: the rights and permissions granted to an individual, which enable access to a computer resource. Authorization is the access rights granted to a user, program or process

- **Privacy:** This means the level of confidentiality and privacy protection that a user is given in a system.

Biometrics controls for security

- Biometrics is a science for determining a person's identity by measuring his/her physiological or behavioral characteristics.
- Now a days, a wide variety of applications require reliable verification scheme to confirm the ID of an individual.
- Biometrics is used as one of the methods for physical access control.

Examples

- Voice
- Fingerprint
- Retina
- Iris
- Signature
- Gait
- Face