INFORMATION SECURITY

Introduction

Dr. Shubhangi Sapkal

- Information – (1) Facts or ideas, which can be represented (encoded) as various forms of data; (2) Knowledge (e.g., data, instructions) in any medium or form that can be communicated between system entities.
- Information Security – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability.

- Confidentiality – Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Integrity – Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity. o Data Integrity – The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. o System Integrity – The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.
- Availability – Ensuring timely and reliable access to and use of information.
- Security Controls – The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a system to protect the confidentiality, availability, and integrity of the system and its information.

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.

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

Apart from this there is one more principle that governs information security programs. This is Non repudiation.

- **Non repudiation –** means one party cannot deny receiving a message or a transaction nor can the other party deny sending a message or a transaction. For example in cryptography it is sufficient to show that message matches the digital signature signed with sender’s private key and that sender could have a sent a message and nobody else could have altered it in transit. Data Integrity and Authenticity are pre-requisites for Non repudiation.

- **Authenticity –** means verifying that users are who they say they are and that each input arriving at destination is from a trusted source.This principle if followed guarantees the valid and genuine message received from a trusted source through a valid transmission. For example if take above example sender sends the message along with digital signature which was generated using the hash value of message and private key. Now at the receiver side this digital signature is decrypted using the public key generating a hash value and message is again hashed to generate the hash value. If the 2 value matches then it is known as valid transmission with the authentic or we say genuine message received at the recipient side
- **Accountability –** means that it should be possible to trace actions of an entity uniquely to that entity. For example as we discussed in Integrity section Not every employee should be allowed to do changes in other employees data. For this there is a separate department in an organization that is responsible for making such changes and when they receive request for a change then that letter must be signed by higher authority for example Director of college and person that is allotted that change will be able to do change after verifying his bio metrics, thus timestamp with the user(doing changes) details get recorded. Thus we can say if a change goes like this then it will be possible to trace the actions uniquely to an entity.

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 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.