Information Assurance and Security

Chapter One

Introduction

November 2022

Introduction

Data

- is the raw material for representing facts, ideas, concepts or any notions we have.
- Data has no meaning by its own and it could be represented by numbers, characters, symbols or word.

Information

- is the processed, well organized, analyzed and interpreted type of data which is meaningful by its own.
- So that we can make any decision or take any action by depending on the information we. have rather that data.
- This is because it is well organized, processed, analyzed and interpreted one.

Characteristics of Information

Availability

- Information is said to be available to an authorized user when and where needed and in the correct format.
- If the information is available 24 hours in 7 days (24/7).

Accuracy

- Free from mistake or error and having the value that the end-user expects.

Authenticity

- Authenticity can be the quality or state of being genuine or original, rather than a reproduction or fabrication

Cont'd

Confidentiality

- The quality or state of preventing disclosure or exposure to unauthorized individuals or systems.

Integrity

- The quality or state of being whole, complete, and uncorrupted.
- The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state.

Information Assurance

- Is the practice of protecting against and managing risk related to the use, storage and transmission of data and information systems.
- It measures those protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Cont'd

Security

- Security concerning information is normally defined by three aspects or goal; confidentiality, integrity and availability.
- It is the quality or state of being secure or save or protected to be free from danger.

Cont'd

Information Security

- covers the tools and processes that organizations use to protect information.
- This includes policy settings that prevent unauthorized people from accessing business or personal information.
- It protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction.
- It is the superset that contains cyber security and network security.
- Information security is achieved by:
  - Procedural Controls
  - Access Controls
  - Technical Controls

Cont'd

Network security

- Network security is the protection of the underlying networking infrastructure from unauthorized access, misuse, or theft.
- This means that a well-implemented network security blocks viruses, malware, hackers, etc. from accessing or altering secure information.
- Network Security is achieved by:
  - Firewall
  - Remote Access VPN
  - Email Security
  - Intrusion Prevention Systems (IPS)

Important concepts in Information Security

Access

- A subject or object ability to use, manipulate, modify or affect another subject's object.

Asset

- The organization resource that is being protected.
- Assets can be either Logical or Physical:
  - Logical assets like web site, information or data and physical assets such as person, computer system.

Attack

- An action taken against a target with the intention of doing harm.

Cont'd

Threat

- A category of objects, persons, or other entities that presents a danger to an asset.

Vulnerability

- A weaknesses or fault in a system or protection mechanism that opens it to attack or damage.
- Some examples of vulnerabilities are a flaw in a software package, an unprotected system port, and an unlocked door.

Loss

- A single instance of an information asset suffering damage or unintended or unauthorized modification or disclosure. When an organization's information is stolen, it has suffered a loss.

Enterprise Security

- Enterprise security involves the various technologies, tactics, and processes used to protect digital assets against unauthorized use, abuse, or infiltration by threat actors.
- Enterprise security includes the protection of data as it flows across networks, including those connecting satellite offices and those that tie data into the general internet.
- Enterprise security systems also cover the people and policies that organizations use to secure their network infrastructure, including assets such as devices.

Enterprise Security Architecture

- Is a comprehensive plan for ensuring the overall security of a business using the available security technologies.
- Enterprise security architecture represents a cohesive design that helps the different pieces of a security infrastructure work well together.
  - If a business has the right tools and resources but uses them incorrectly, it most likely does not get the intended results.

Benefits of Enterprise Security Architecture

- Threat Mitigation: identify and resolve critical threats facing your org.
- Increased Confidence: give confidence to executives and other stakeholders that security requirements are met.
- Asset validation: defines and validate information
- Implement data protection
- Improve assurance for critical transactions

Security Goals

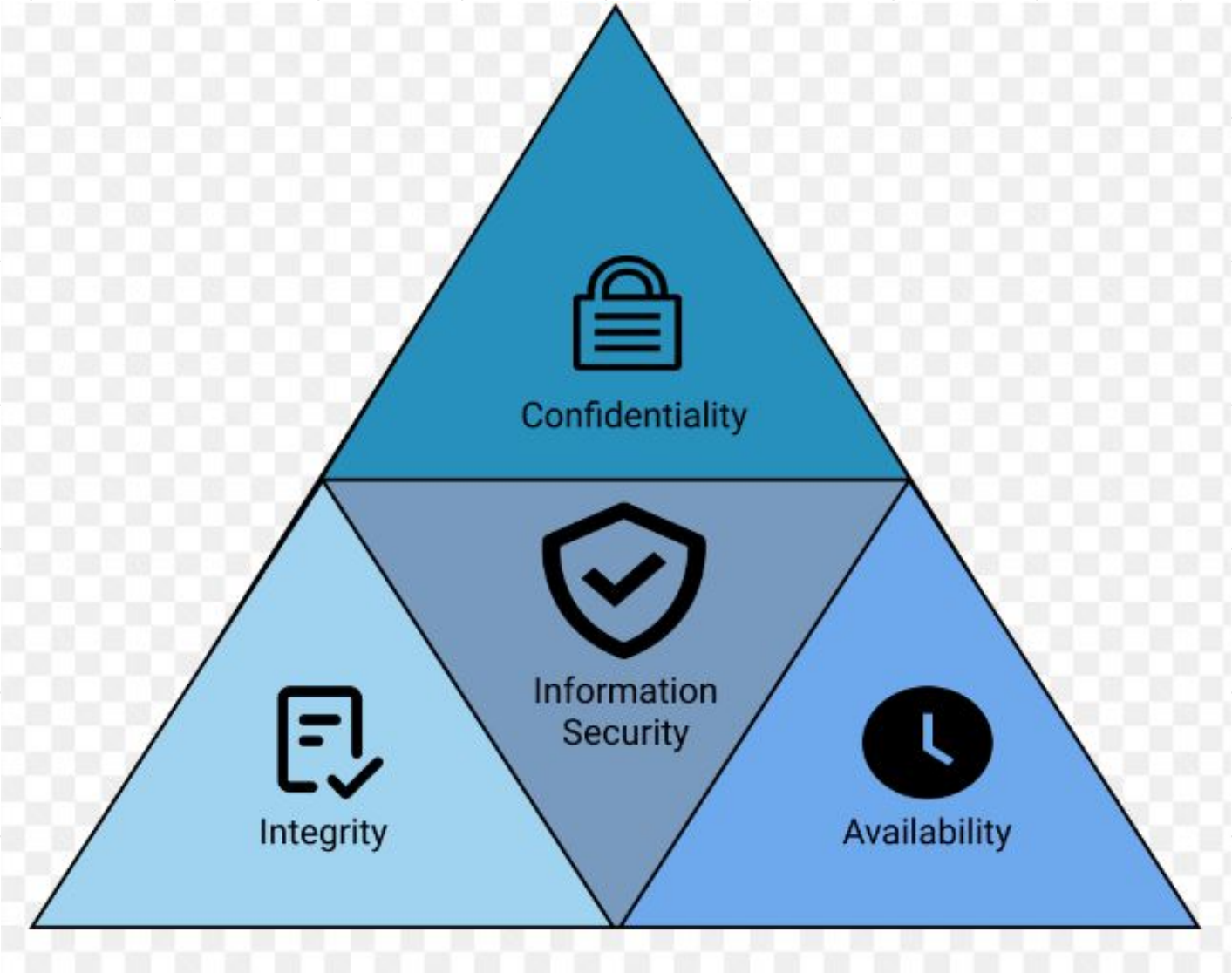
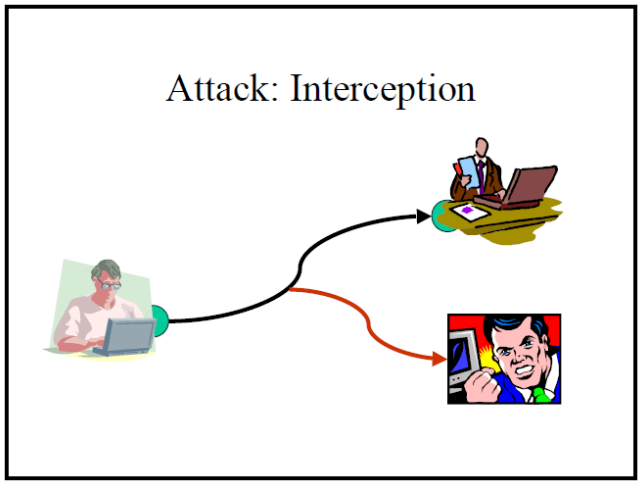


Figure: Security goal

Cont'd

Confidentiality

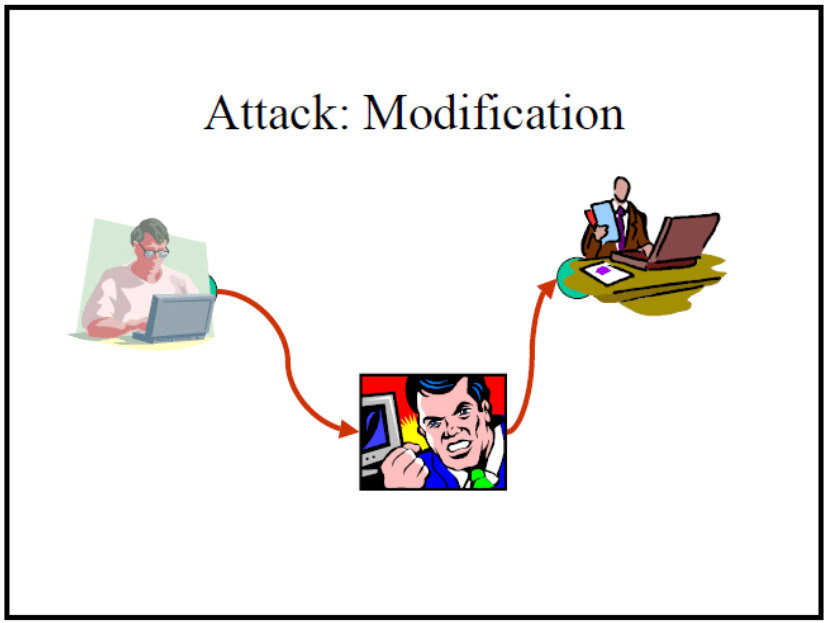
- Keep data and communication secret.
- To ensure data remains private.
  - Examples: Snooping and Traffic analysis
- Confidentiality is usually achieved by:
  - Encryption
  - Access control
  - Authentication



Cont'd

Integrity

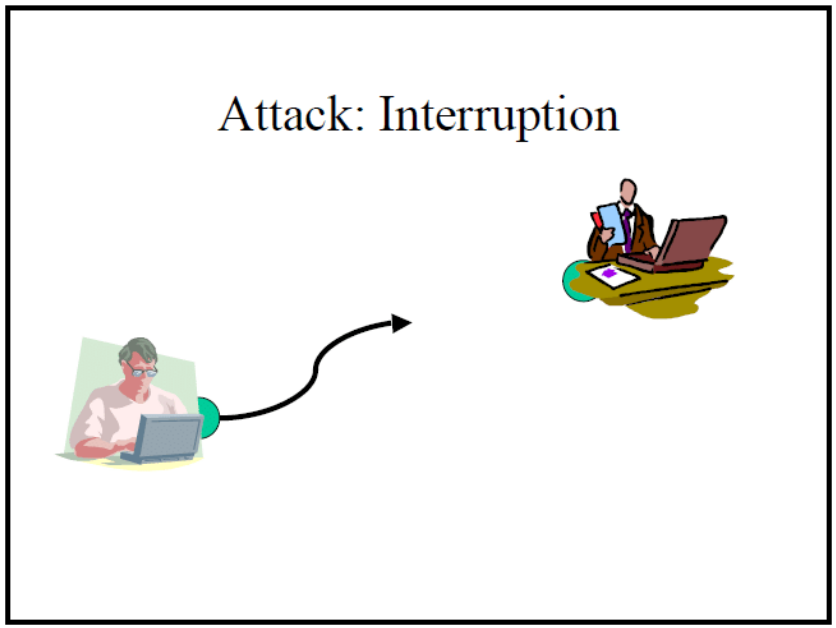
- To ensure data is protected from accidental or deliberate (malicious) modification.
  - Examples: Modification, Masquerading, Replaying, and repudiation
- Tools for integrity
  - Backups
  - CheckSums



Cont'd

Availability

- Information should be available to authorized users when it is needed.
  - Examples: Denial of service attack
- Tools for Availability
  - Physical Protections
  - Computational Redundancies



Cyber Attacks

- A cyber attack is any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage.
- Cyber attacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems.

Some Cyber Attacks

Ransomware

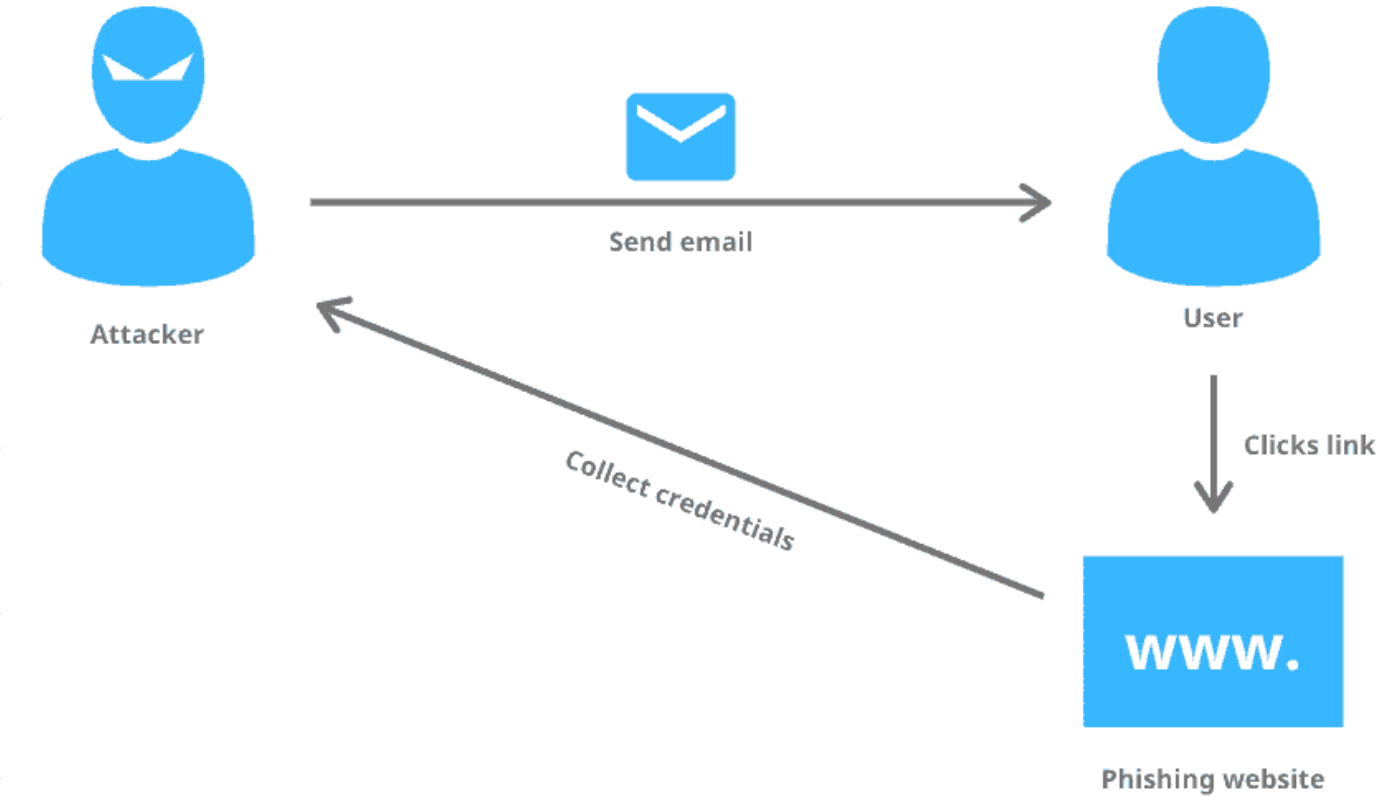
- This is a form of malware (malicious software) that attempts to encrypt (scramble) your data and then extort a ransom to release an unlock code.
- Most ransomware is delivered via malicious emails

Figure: Ransomware

Cont'd

Phishing

- Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.



Cont'd

Data leakage

- The unauthorized transmission of data from an organization to any external source.
- This data can be leaked physically or electronically via hard drives, USB devices, mobile phones, etc., and could be exposed publicly or fall into the hands of a cyber criminal.

Hacking

- Hacking refers to activities that seek to compromise digital devices, such as computers, smartphones, tablets, and even entire networks.

Cont'd

Insider threat

- An insider threat is a security risk that originates from within the targeted organization.
- It typically involves a current or former employee or business associate who has access to sensitive information or privileged accounts within the network of an organization, and who misuses this access.

Cyber Defense

- Cyber defense can be any avoidance or counter measure that is undertaken to overcome the threat that is occured over internet or by a system.
- Cyber defense focuses on preventing, detecting and providing timely responses to attacks or threats so that no infrastructure or information is tampered with.
- With the growth in volume as well as complexity of cyber attacks, cyber defense is essential for most entities in order to protect sensitive information as well as to safeguard assets.