Chapter One

Information Assurance and Security

Introduction

What is Information Assurance?

- Information Assurance is defined as the set of measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality.
- **Information assurance (IA)** is assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes.

Continued...

a risk management plan.

- **Risk management plan proposes countermeasures .**

1. Detection
2. Accepting
3. Mitigating/ justify
4. Response to threats.
5. Eliminating
6. Considers prevention
7. Transferring the risks

What is countermeasure?

- In computer security a **countermeasure** is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.
- It include technical tools such as firewalls and anti-virus software, policies and procedures.

Five Information Assurance pillars

- The five information assurance (IA) pillars are availability, integrity, authentication, confidentiality, and non-repudiation.
- These pillars and any measures taken to protect and defend information and information systems, to include providing for the restoration of information systems, constitute the essential underpinnings for ensuring trust and integrity in information systems.
- The cryptologic components of information assurance primarily address the last four pillars of integrity, authentication, confidentiality, and non-repudiation.

Continued…

- These pillars are applied in accordance with the mission needs of particular organizations.

1. **integrity,** which means protecting against improper information modification or damage, and includes ensuring information non repudiation and authenticity;

2. **confidentiality**, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;

3. **availability**, which means ensuring timely and reliable access to and use of information

Information Assurance strategy

- Cyber security awareness and education;
- Strong cryptography
- Good security-enabled commercial information technology;
- An enabling global Security Management Infrastructure; and
- A civil defence infrastructure equipped with an attack sensing and warning capability and coordinated response mechanism

Difference between information protection and information assurance in Data Protection

- **Information Assurance (AI):** Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.
- **Information protection :-**The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide

Computer security

- The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.
- The term computer system security means the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively.

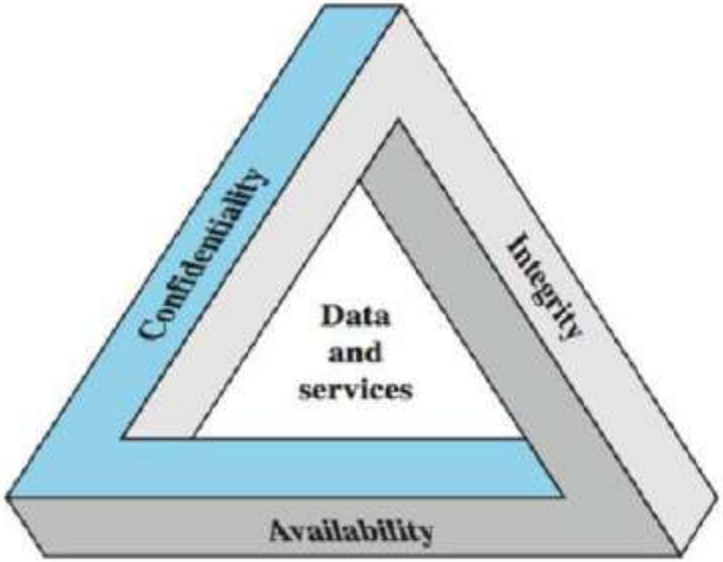
Continued...

- The strategies and methodologies of computer security often differ from most other computer technologies because of its somewhat elusive objective of preventing unwanted computer behaviour instead of enabling wanted computer behaviour.
- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

Why Security is needed ?

- To protect Damage or destruction of computer systems, and internal data.
- Protect Loss of sensitive information to hostile parties.
- Protect Use of sensitive information against the organization's customers which may result in legal action by customers
- Protect Damage of an organization data

Continued…



Security Goals

- C.I.A.

Integrity
Confidentiality
Availability

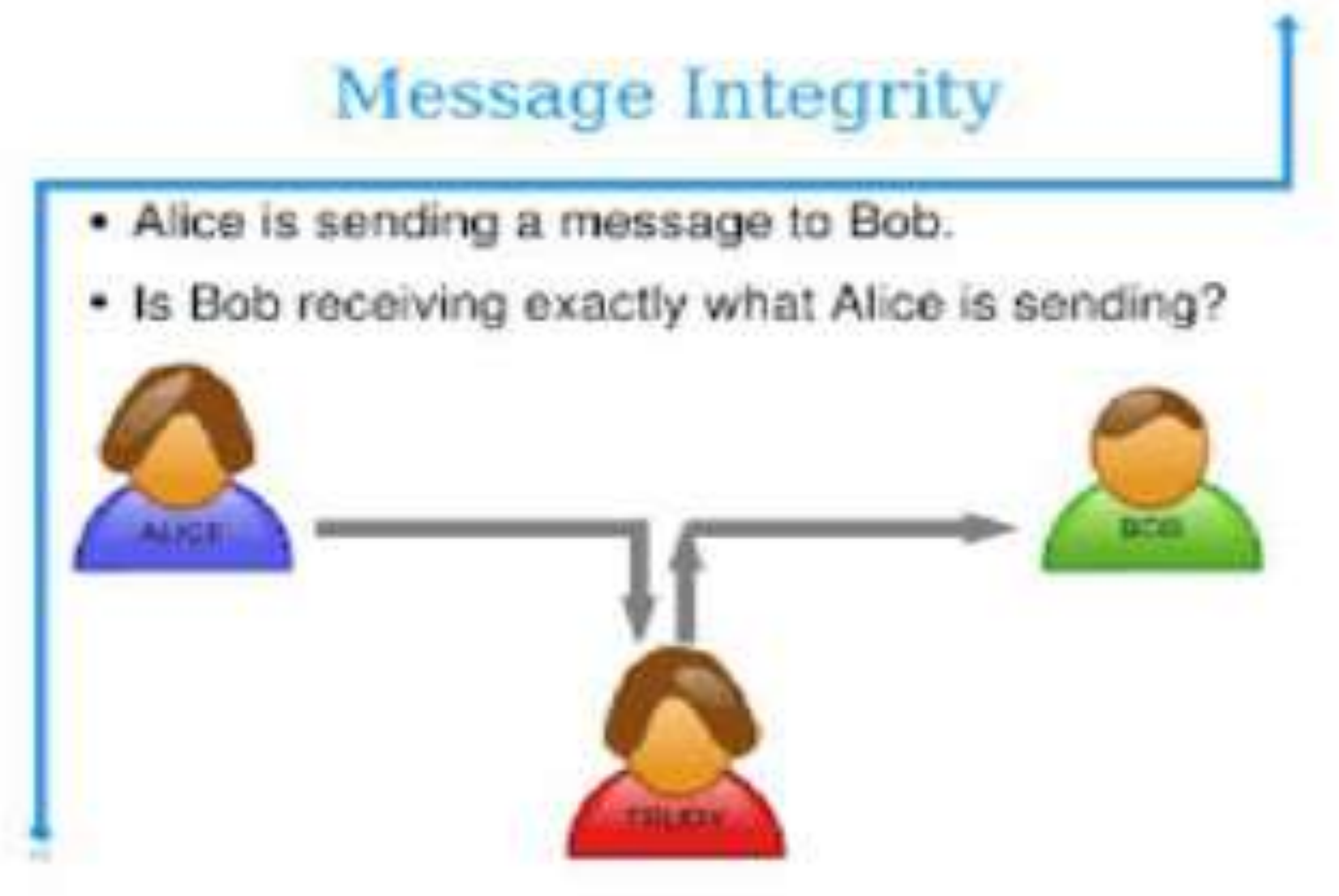
- **Fig 1: Key Security Concepts**

Confidentiality

Continued…

- **Confidentiality** is a set of rules that limits access to information.
- Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems.
- Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it.
- Training can help familiarize authorized people with risk factors and how to guard against them. Further aspects of training can include strong passwords and password-related best practices and information about social engineering methods.

Integrity



Message Integrity

- Alice is sending a message to Bob.
- Is Bob receiving exactly what Alice is sending?

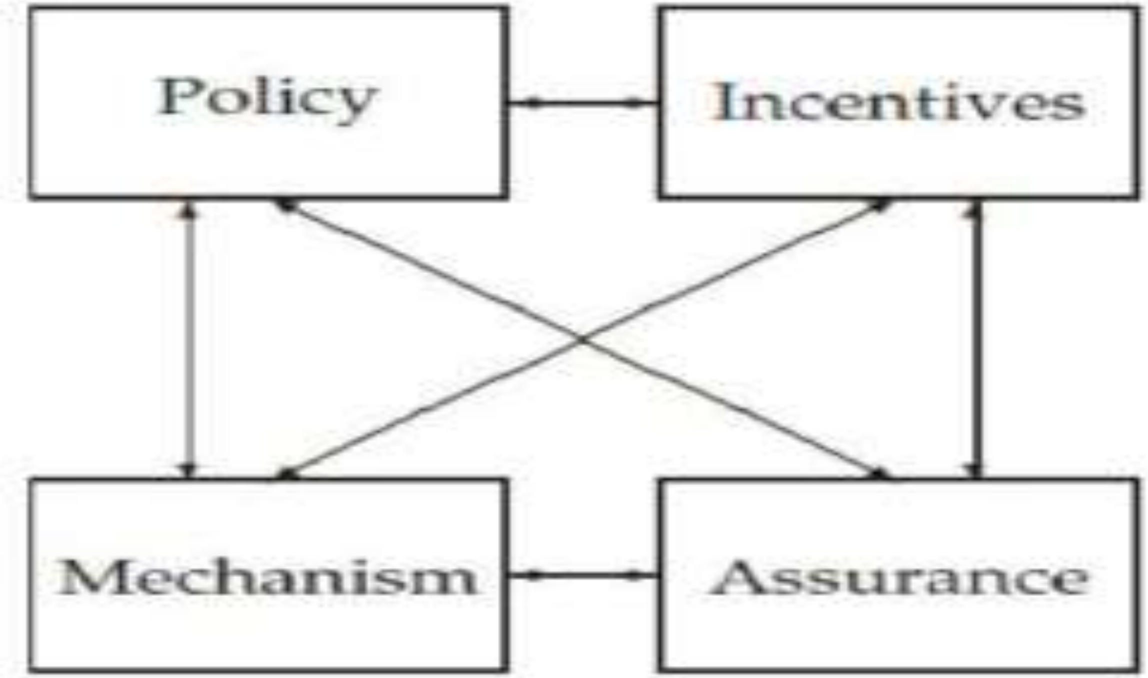
Availability

- It means that assets are accessible to authorized parties at appropriate times.
- Availability is very much a concern beyond the traditional boundaries of computer security.
- We want to ensure that a malicious attacker cannot prevent legitimate users from having reasonable access to their systems.

What Is Enterprise security?

- Enterprise security is about building systems to detect malice problems , error, or mischance. As a discipline, it focuses on the tools, processes, and methods needed to design, implement, and test complete systems, and to adapt existing systems as their environment evolves.
- Enterprise security requires cross-disciplinary expertise, ranging from cryptography and computer security through hardware tamper-resistance and formal methods to a knowledge of economics, applied psychology, organizations and the law.

Enterprise Security Analysis Framework



- **Figure 1: Enterprise Security Analysis Framework**

Continued...

- Good Enterprise security requires four things to come together.
- 1. **Policy**: what you're supposed to
- 2. **Mechanism**: the ciphers, access controls, hardware tamper-resistance and other machinery that you assemble in order to implement the policy.
- 3. **Assurance**: the **amount of confidence** you can place on each particular mechanism.
- **4. Incentive**: the motive that the people guarding and maintaining the system have to do their job properly, and also the motive that the attackers have to try to defeat your policy.
- All of these interact

Enterprise Security Architecture: Establishing the Business Context

- A **business-driven approach** to enterprise security architecture means that security is about enabling the objective of an organization by controlling operational risk.
- This business-driven approach becomes a key differentiator to existing security practices that are focused solely on identifying threats to an enterprise and technical vulnerabilities in IT infrastructure, and subsequently implementing controls to mitigate the risks introduced.
- A purely **threat-based approach** to risk management fails to enable effective security and business operations. The term security will carry very different meanings to different organizations.
- For example, consider security as it relates to a **military organization** and security related to an **online retailer** that processes credit card information.

Cyber Defense

- **Definition - What does Cyber Defense mean?**
- Cyber defence is a computer network defence mechanism which includes response to actions and critical infrastructure protection and information assurance for organizations, government entities and other possible networks.

Cyber defence focuses on

- 1. preventing, detecting and providing timely responses to attacks or threats
- 2. Prevent complexity of cyber-attacks,
- 3. protect sensitive information as well as to safeguard assets.

Continued…

- 4. It helps in devising and driving the strategies necessary to counter the malicious attacks or threats.
- 5. It reducing the appeal of the environment to the possible attackers,
- 6. Cyber defence also carries out technical analysis to identify the Threat
- 7. It helps in enhancing the security strategy utilizations and resources in the most effective fashion.
- 8. Cyber defence also helps in improving the effectiveness of the security resources and security expenses, especially in critical locations.
- 9. Cyber Defense protects your most important business assets against attack

Thank You!