Unit 1- Introduction to Cybersecurity

This unit introduces the main concepts of cybersecurity, its aim, objectives, and requirements. The assets that require security measures are described together with the types of potential threats and attacks.

At the end of the unit, the learner should be able to:

- Describe the main security requirements: confidentiality, integrity, and availability
  - Discuss the categories of threats and attacks
- List the fundamental functional security requirements of digital information systems
- Explain the 13 fundamental principles of security design
- Discuss the use of attack surfaces and attack trees
- Identify the main international and local organizations and standards related to cybersecurity and their roles

Target Audience: Third Year Students - BSc Software Engineering, BSc Computer Science

1. Cybersecurity: Definition, Aims and Objectives

Cybersecurity is a broad term that refers to the collection of interrelated technologies, processes, and practices designed to protect digital assets (e.g. computer networks, devices, programs, and data) from attack, damage, or unauthorized access. Cybersecurity is also sometimes referred to as computer security or information security though the terms may have different meanings.

Cybersecurity aims to **discourage**, **prevent**, **detect**, and **neutralize** security violations that are involved in the storage and transmission of information. It concerns the protection of digital assets such as hardware, software, firmware, data/information, and telecommunications

The fundamental **objectives** of cybersecurity (often referred to as the **CIA triad**) are:

1. Confidentiality
2. Integrity
3. Availability

Confidentiality is the assurance that access to assets is granted to authorized parties only thus preserving the privacy of the assets.

Integrity is the preservation of consistency, accuracy, and trustworthiness of an asset throughout its lifetime.

Availability is the assurance that a system shall be consistently and readily accessible throughout the time it was designed to be available.

In addition to confidentiality, integrity, and availability, two more aspects of security must be catered for: authenticity and accountability.

Authenticity is the property of an asset or the identity of entity (a user, device or system) being genuine, verifiable, and trustworthy.

Accountability is an aspect of security goals whereby any action performed in an information system is traceable and its responsibility is binding to the executor or enabler.

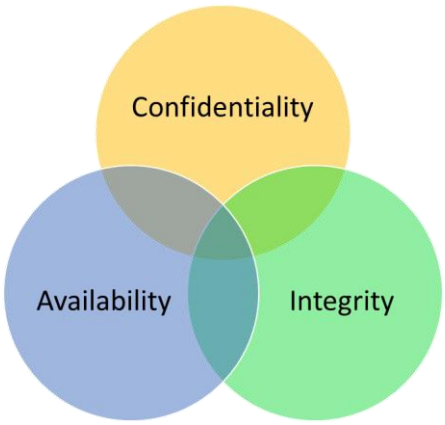

Figure 1.1: The CIA Security Triad

Confidentiality, Integrity and Authenticity can be provided by algorithms (cryptographic primitives) from the field of Cryptography. A simplified cryptographic model is depicted in figure 1.2 whereby a sender is attempting to send a message over an unsecure channel.

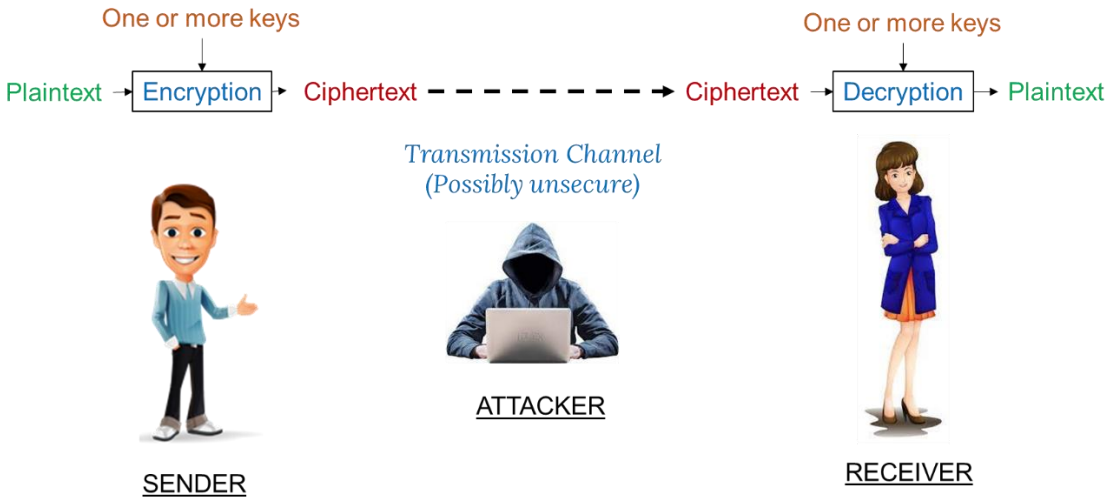

Figure 1.2: A Simplified Cryptographic Model

2. Types of Cyber Attacks

There are two broad categories of cyber attacks: Passive and Active.

A **passive attack** attempts to gather, disclose or use information from the system but does not affect the system resources.

Passive attacks are in the nature of eavesdropping on or monitoring transmissions. Passive attacks are difficult to detect.

Two types of passive attacks are:

1. The disclosure of message contents
2. Traffic Analysis

An **active attack** attempts to modify or destroy system resources or affect the system's operation.

Four categories of active attacks are:

1. Masquerade - the attacker impersonates another entity
2. Replay - retransmission of a passive data capture to produce an unauthorized effect
3. Message Modification
4. Denial-of-Service - Prevents or inhibits normal system function

3. Fundamental Principles of Security Design

System and software developers need to follow some guidelines when designing their products for security. Despite years of research and development, it has not been possible to develop security design and implementation techniques that systematically exclude security flaws and prevent all unauthorized actions. So, we adopt general guidelines for security design. Security design principles are foundational guidelines for building resilient systems. Proposed by Jerome Saltzer and Michael Schroeder in 1975, these principles mitigate vulnerabilities by structuring systems to inherently resist attacks. While technologies evolve, these 13 axioms remain timeless.

1. Economy of mechanism
2. Fail-safe defaults
3. Complete mediation
4. Open design
5. Separation of privilege
6. Least privilege
7. Least common mechanism
8. Psychological acceptability
9. Work Factor
10. Compromise Recording
11. Layering
12. Diversity of Defence
13. Modularity

1. Economy of Mechanism:
Principle: Keep security designs simple and small.
Example: Use microservices instead of monolithic systems to isolate security functions.
Why: Complex systems have more hidden flaws; simplicity eases verification.

2. Fail-Safe Defaults
Principle: Default to denying access unless explicitly permitted.
Example: Firewalls block all traffic by default; only whitelisted applications run in secure environments.
Why: Prevents unauthorized access when configurations are incomplete.

3. Complete Mediation
Principle: Check every access request for authorization.
Example: Re-validate permissions for each file read (not just on initial access).
Why: Prevents attackers from exploiting cached permissions.

4. Open Design
Principle: Security should not rely on obscurity; algorithms should be public.
Example: AES and RSA are open standards; keys provide secrecy, not hidden algorithms.
Why: Public scrutiny improves robustness; secrecy shifts to keys.

5. Separation of Privilege
Principle: Require multiple conditions for critical access.
Example: Two-factor authentication (password + biometric) or dual-key nuclear launch codes.
Why: Raises the attack barrier; single failures won't compromise security.

6. Least Privilege
Principle: Grant users/processes only the minimum permissions necessary to perform their tasks.
Example: A web server should not have root access; a database user should only read/write to specific tables.
Why: Limits damage from compromised accounts or malware.

7. Least Common Mechanism
Principle: Minimize shared resources between users hence fostering mutual security.
Example: Isolate VM instances in cloud environments; avoid shared system directories.
Why: Prevents cross-account attacks (e.g., side-channel exploits).

8. Psychological Acceptability
Principle: the security mechanisms should not interfere unduly with the work of users, while at the same time meeting the needs of those who authorize access .
Example: Auto-fill password managers reduce friction while improving password strength.
Why: Unintuitive security leads to workarounds (e.g., weak passwords).

9. Work Factor
Principle: Cost of bypassing security should exceed the attacker's gain.
Example: AES-256 encryption requires 2^{256} operations to brute-force—infeasible for most threats.

Why: Aligns defences with realistic adversary capabilities.

10. Compromise Recording
Principle: Log evidence of breaches even if prevention fails.
Example: Audit trails tracking file access; honeypots that capture attack methods.
Why: Enables forensic analysis and damage control.

11. Layering (Defence in Depth)
Principle: Use multiple, diverse security controls, overlapping protection approaches addressing the people, technology, and operational aspects of information systems.
Example: Firewall + IDS + encryption + application sandboxing.
Why: Single layers fail; redundancy increases resilience.

12. Diversity of Defence
Principle: Employ different security mechanisms at each layer.
Example: Mixing different kinds of security measures.
Why: Avoids single-point failures; thwarts exploits targeting one technology.

13. Modularity
Principle: Isolate components so failures don't cascade.
Example: Microservices architecture with API gateways; hardware security modules (HSMs).
Why: Contains breaches; simplifies updates and testing.

Attack Surfaces

An **attack surface** is a list of all the possible ways an attacker can use the reachable and exploitable vulnerabilities of a system.

The attack surfaces may be classified into:

1. **Network attack surface**, which comprises the network environment of an organization.
2. **Software attack surface**, which includes all the applications and operating systems or utilities used within an organization.
3. **Human attack surface**, which involves human errors and human users being tricked into voluntarily giving away access to sensitive information.

Some examples of attack surfaces are open ports on servers, web forms for data entry, and naive and empathetic users.

A thorough **attack surface analysis** is a good technique for the assessment of the severity and scale of threats to a system. Securing such a system involves reducing the attack surface to a minimum.

Attack Trees

An **attack tree** is a tree diagram that depicts the potential ways the vulnerabilities of the asset(s) of a system may be exploited.

The **root node** of an attack tree represents the security incident (i.e. the goal of the attack). The **branches** from the root node (and sub-nodes) represent the different ways that the attack could reach that goal. The **final nodes** (leaf or end nodes) represent the ways the attack may be initiated.

Attack trees can be used to effectively use the information to identify attack patterns.

4. Dimensions of Cybersecurity

Cybersecurity is a multidisciplinary mosaic. encompassing multiple interconnected dimensions that collectively protect systems, data, and operations. Here is a structured breakdown of the core dimensions of cybersecurity as shown in table 4.1.

Table 4.1: Core Dimensions of Cybersecurity

Technological : Network security Operating system security Application security Cloud security Cryptography	**Human and Social :** Safety awareness User training Access and identity management User behaviour Social engineering	**Legal and Regulatory:** Data protection laws (e.g. GDPR, CCPA) Industry regulations (e.g. HIPAA, PCI DSS) Cybercrime legislation Digital rights
Economic and Financial : Costs of security incidents Cybersecurity insurance Investments in cybersecurity Economic impact of attacks	**Policy and Governance :** National cybersecurity strategies International cooperation Role of government agencies Governance of emerging technologies	**Operational :** Security incident management Business continuity planning Penetration and vulnerability testing Patch management
Emerging Technologies : Integrating artificial intelligence Use of Blockchain in cybersecurity Quantum cybersecurity Connected object security	**Information and Communication :** Sharing information on threats Communication during cybersecurity crisis Security-related public relations Internal and external communication	**Ethics and Privacy :** Respect for user privacy Ethical use of data Liability in the event of a security breach Balancing security and personal freedom
Environmental : Energy and sustainability in data centres Environmental impact of cybersecurity technologies Ecological practices in the development/use of cybersecurity solutions	**International Collaboration :** Information sharing between countries Cooperation in combating cross-border threats Development of global standards and best practices	

5. Local and International Regulators of Cybersecurity

There are several international organizations that are involved in the development of security norms and standards.

Some of the international Standards Organizations relevant to Cybersecurity are:

- National Institute of Standards and Technology (NIST)
  - NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private sector innovation
- Internet Society (ISOC)
  - ISOC is a professional membership society that provides leadership in addressing issues that confront the future of the Internet and is the organization home for the groups responsible for Internet infrastructure standards
- International Telecommunication Union (ITU-T)
  - ITU is a United Nations agency in which governments and the private sector coordinate global telecom networks and services
- International Organization for Standardization (ISO)
  - ISO is a non-governmental organization whose work results in international agreements that are published as International Standards

Each country may have its own national and local organizations and agencies which govern the standards and laws of Cybersecurity within a particular region or field. Can you list the authorities responsible for cybersecurity in your country?