COLLEGE of COMPUTER STUDIES

ITA 216 Platform Security

Introduction to Platform Security

Ms. Kezia Abegail T. Velasco

SY 2024-2025

What is Platform Security?

Platform Security refers to the set of strategies, tools, and policies used to protect the hardware, operating system, and software environments from cyber threats and unauthorized access.

Scope:

- Covers physical devices, virtualization layers, OS, applications, and APIs
- Applies to mobile, cloud, desktop, IoT, and enterprise systems

Importance of Platform Security

Platforms are the foundation for applications and services. A breach at the platform level can compromise everything built on it.

Benefits:

- Protects sensitive data from theft or loss
- Prevents downtime that affects productivity
- Ensures compliance with security regulations (e.g., GDPR, HIPAA)
- Maintains user trust in the system or service

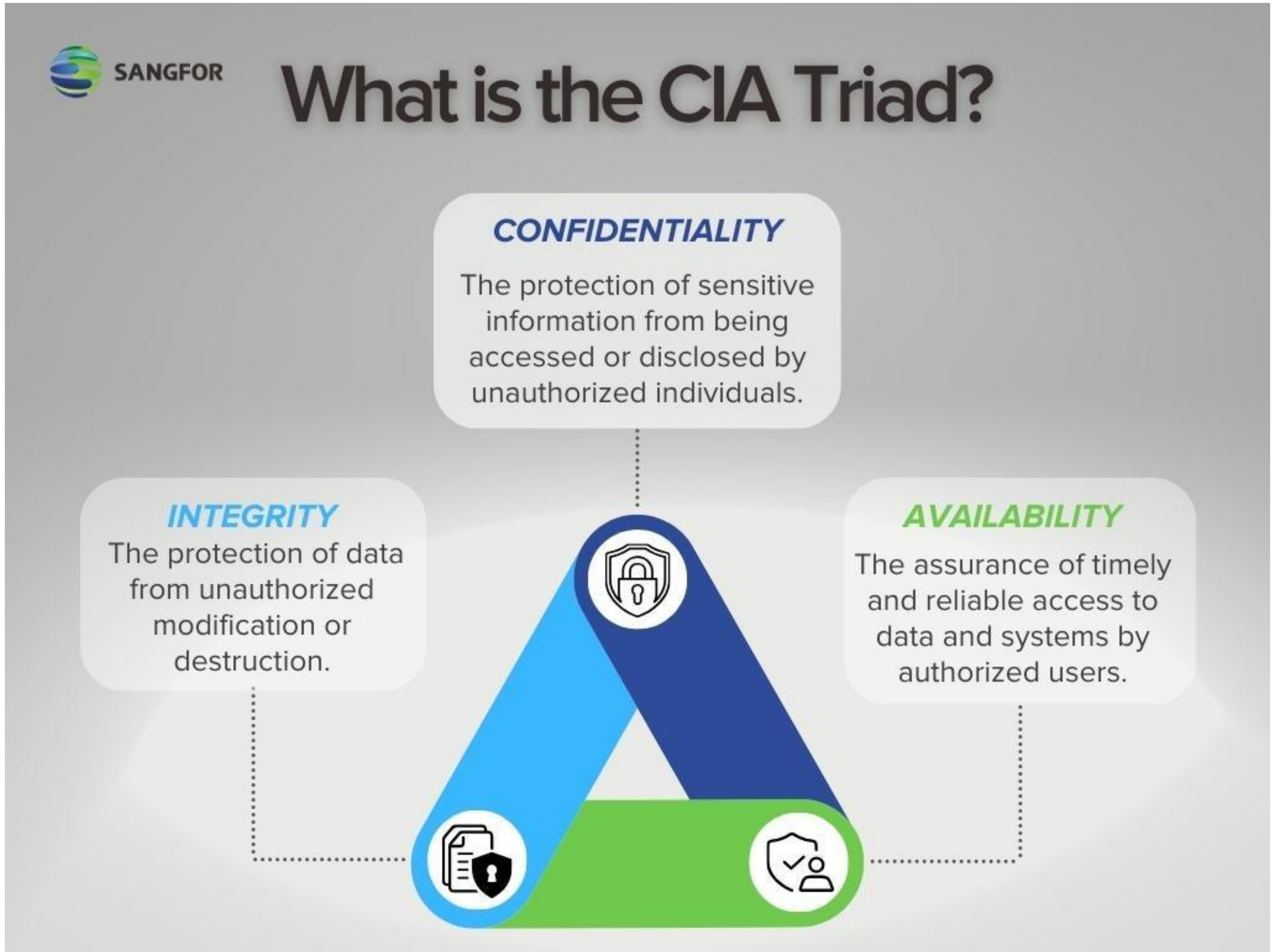
Common Threats to Platforms

- **Malware** – Viruses, ransomware, spyware targeting system files
- **Privilege Escalation** – Attackers gaining admin-level access
- **Zero-Day Exploits** – Attacks exploiting unpatched vulnerabilities
- **Rootkits** – Malicious code hidden deep in the OS
- **Firmware Attacks** – Compromising the BIOS/UEFI or device drivers
- **Insider Threats** – Employees misusing access rights

Layers of Platform Security

- **Physical Security:** Protecting hardware from theft or tampering
- **Firmware & Boot Security**: Secure boot, BIOS/UEFI passwords
- **Operating System Security**: Patch management, user privilege control
- **Application Security**: Sandboxing, code signing, app permissions
- **Network Security**: Firewalls, VPNs, intrusion detection/prevention
- **Data Security**: Encryption at rest and in transit

The CIA Triad



SANGFOR

What is the CIA Triad?

CONFIDENTIALITY

The protection of sensitive information from being accessed or disclosed by unauthorized individuals.

INTEGRITY

The protection of data from unauthorized modification or destruction.

AVAILABILITY

The assurance of timely and reliable access to data and systems by authorized users.

Confidentiality

security professional’s obligation is to regulate access—protect the data that needs protection, yet permit access to authorized individuals.

- **Personally Identifiable Information (PII)** It pertains to any data about an individual that could be used to identify them.
- **Protected Health Information (PHI)** , which is information regarding one’s health status,
- **classified or sensitive information**, which includes trade secrets, research, business plans and intellectual property.

Integrity

measures the degree to which something is whole and complete, internally consistent and correct. The concept of integrity applies to:

- information or data
- systems and processes for business operations
- organizations
- people and their actions

Integrity

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.

System Integrity – The quality that the system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

Availability

- can be defined as (1) timely and reliable access to information and the ability to use it, and (2) for authorized users, timely and reliable access to data and information services.

Authentication

- The process of verifying or proving the user’s identification.

There are three common methods of authentication:

1. **Something you know**: Passwords or passphrases
2. **Something you have**: Tokens, memory cards, smart cards
3. **Something you are**: Biometrics , measurable characteristics

Methods of Authentication

Types of Authentication

1. Single-Factor Authentication (SFA)
2. Multi-Factor Authentication (MFA)

Non-repudiation

- legal term and is defined as the protection against an individual falsely denying having performed a particular action

Privacy

- The right of an individual to control the distribution of information about themselves

Example of laws governing privacy:

- **General Data Protection Regulation (GDPR)** applies to all organizations, foreign or domestic, doing business in the EU or any persons in the EU.

COLLEGE *of* COMPUTER STUDIES

Understand the Risk Management Process

Information Security Risk

- potential adverse impacts that result from the possibility of unauthorized access, use, disclosure, disruption, modification or destruction of information and/or information systems.

Risk Management Terminology

- An ***asset*** is something in need of protection. (anything of value, includes tangible and intangible)
- A ***vulnerability*** is a gap or weakness in those protection efforts. (weakness)
- A ***threat*** is something or someone that aims to exploit a vulnerability to thwart protection efforts.

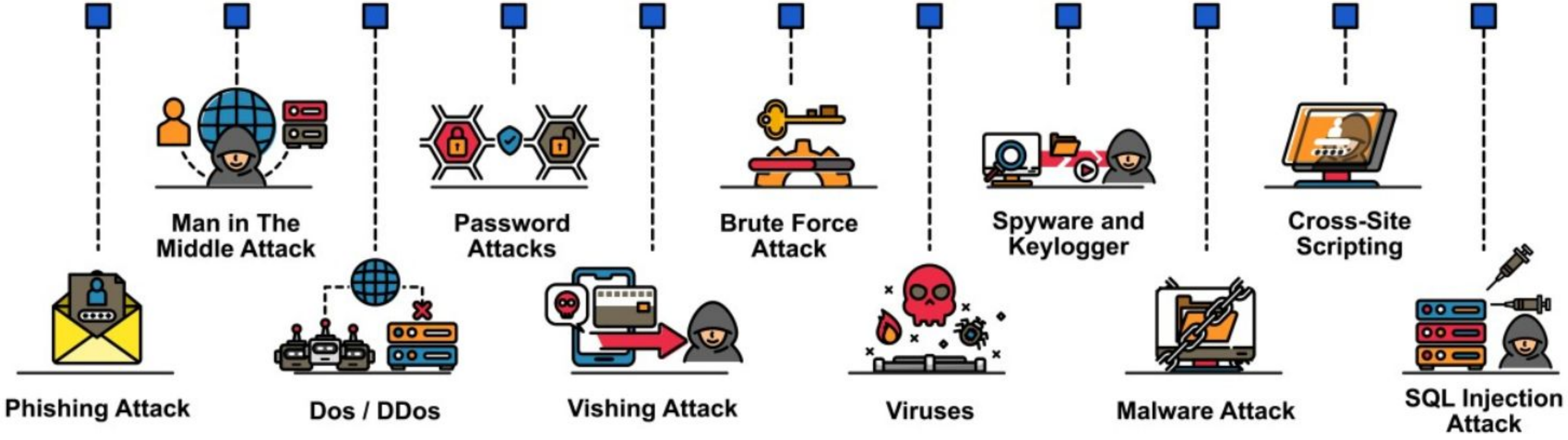
Example:

Tourists are popular targets for pickpockets. The existence of pickpockets in a crowded tourist spot is a threat to the people gathered there. That threat applies to everyone in the vicinity, even other pickpockets. If you are in the vicinity and the pickpocket has identified you as a target, you are facing a threat actor whether you know it or not. The approach and technique taken by the pickpocket is their threat vector.

Threat Actors

- **Insiders** (either deliberately, by simple human error, or by gross incompetence).
- **Outside individuals or informal groups** (either planned or opportunistic, discovering vulnerability).
- **Formal entities that are nonpolitical** (such as business competitors and cybercriminals).
- **Formal entities that are political** (such as terrorists, nation-states, and hacktivists).
- **Intelligence or information gatherers** (could be any of the above).
- **Technology** (such as free-running bots and artificial intelligence , which could be part of any of the above).

CYBER SECURITY ATTACKS



Phishing Attack

Man in The Middle Attack

Dos / DDos

Password Attacks

Vishing Attack

Brute Force Attack

Viruses

Spyware and Keylogger

Malware Attack

Cross-Site Scripting

SQL Injection Attack

Vulnerabilities

- An inherent weakness or flaw in a system or component, which, if triggered or acted upon, could cause a risk event to occur.

Risk Assessment

- defined as the process of identifying, estimating and prioritizing risks to an organization’s operations (including its mission, functions, image and reputation), assets, individuals, other organizations and even the nation

Risk Treatment

- relates to making decisions about the best actions to take regarding the identified and prioritized risk.
- The decisions made are dependent on the attitude of management toward risk and the availability — and cost — of risk mitigation.

Risk Treatment

1. **Avoidance**. The decision to attempt to eliminate the risk entirely.
2. **Acceptance.** Taking no action to reduce the likelihood of a risk occurring.
3. **Mitigation.** Most common type of risk management and includes taking actions to prevent or reduce the possibility of a risk event or its impact.
4. **Risk transference.** is the practice of passing the risk to another party, who will accept the financial impact of the harm resulting from a risk being realized in exchange for payment.