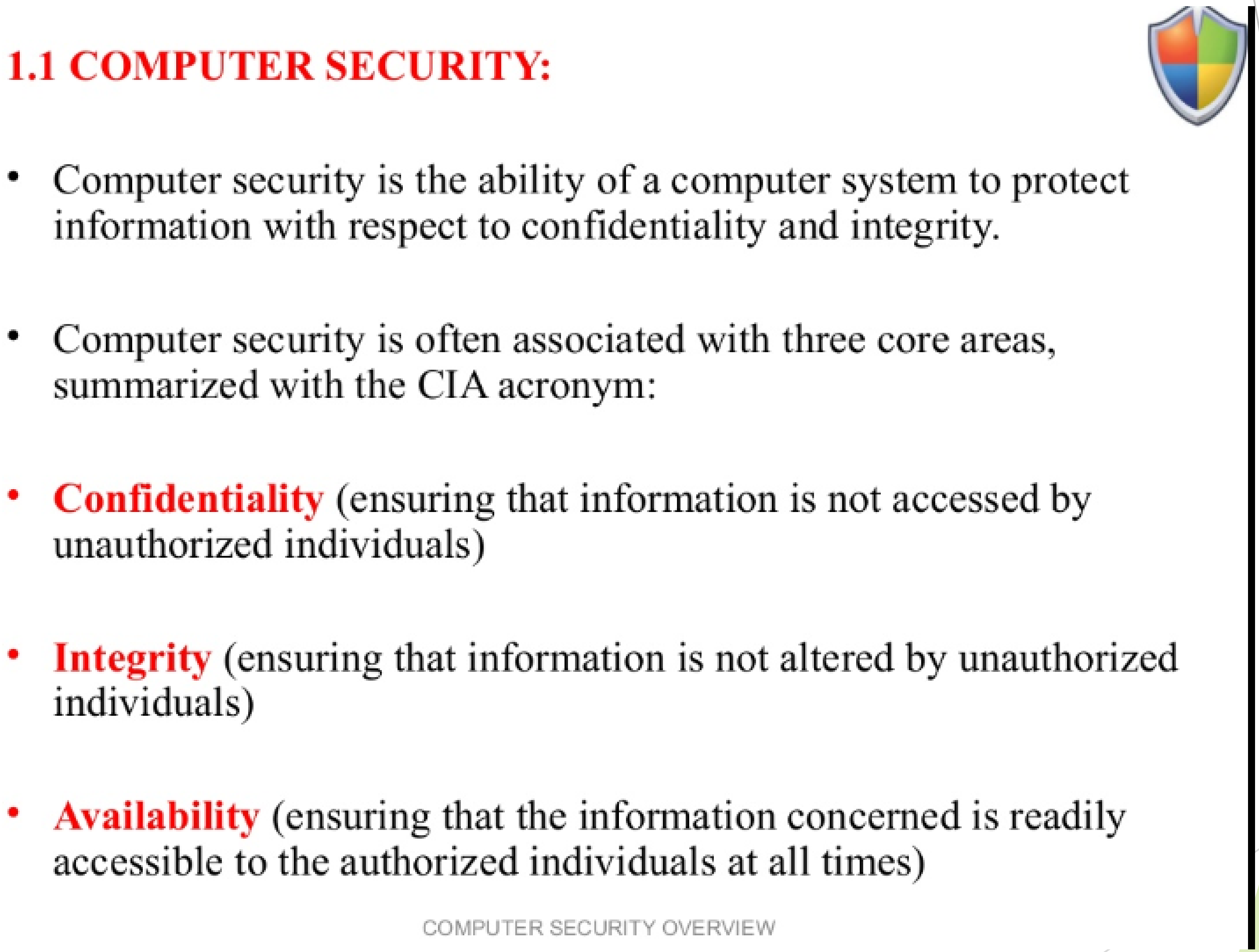
Computer System Security

(KNC-301)

COMPUTER SECURITY

COMPUTER SECURITY - OVERVIEW



1.1 COMPUTER SECURITY:

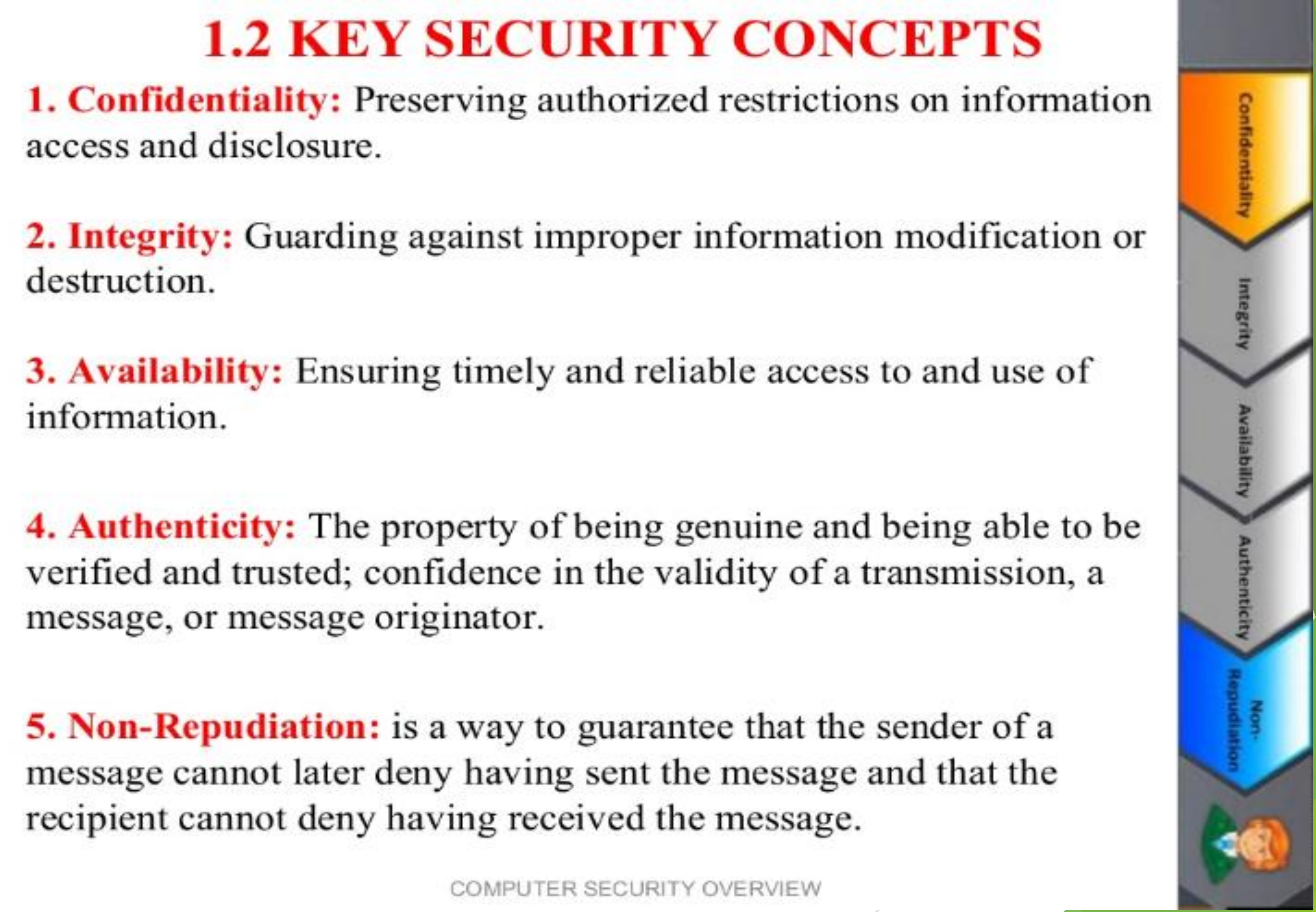
- Computer security is the ability of a computer system to protect information with respect to confidentiality and integrity.

- Computer security is often associated with three core areas, summarized with the CIA acronym:

- **Confidentiality** (ensuring that information is not accessed by unauthorized individuals)

- **Integrity** (ensuring that information is not altered by unauthorized individuals)

- **Availability** (ensuring that the information concerned is readily accessible to the authorized individuals at all times)



1.2 KEY SECURITY CONCEPTS

1. Confidentiality: Preserving authorized restrictions on information access and disclosure.

2. Integrity: Guarding against improper information modification or destruction.

3. Availability: Ensuring timely and reliable access to and use of information.

4. Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.

5. Non-Repudiation: is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

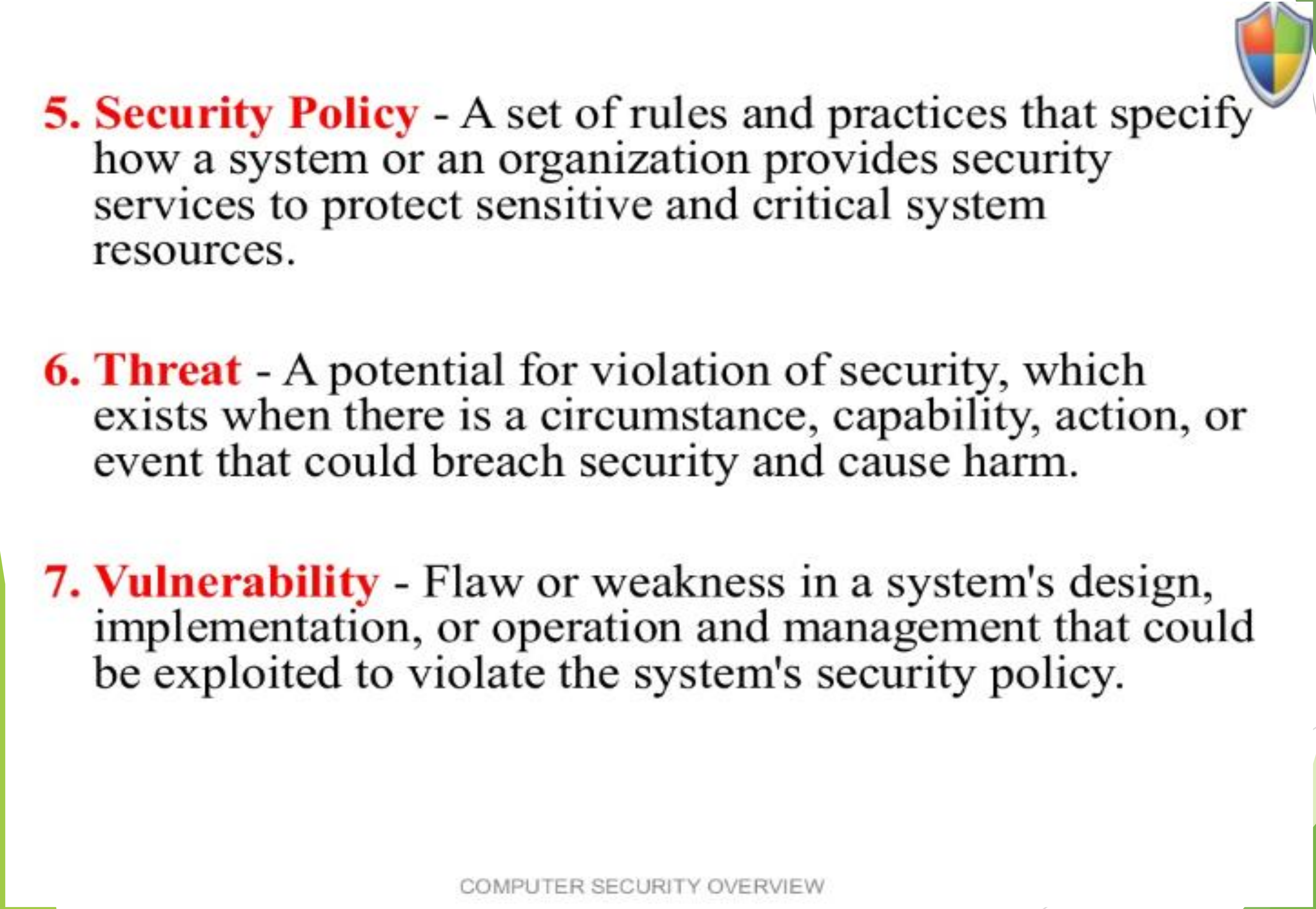
1.3 SECURITY TERMINOLOGY

1. Adversary (threat agent) - An entity that attacks, or is a threat to, a system.

2. Attack -An assault on system security that derives from an intelligent threat; a deliberate attempt to evade security services and violate security policy of a system.

3. Countermeasure - 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.

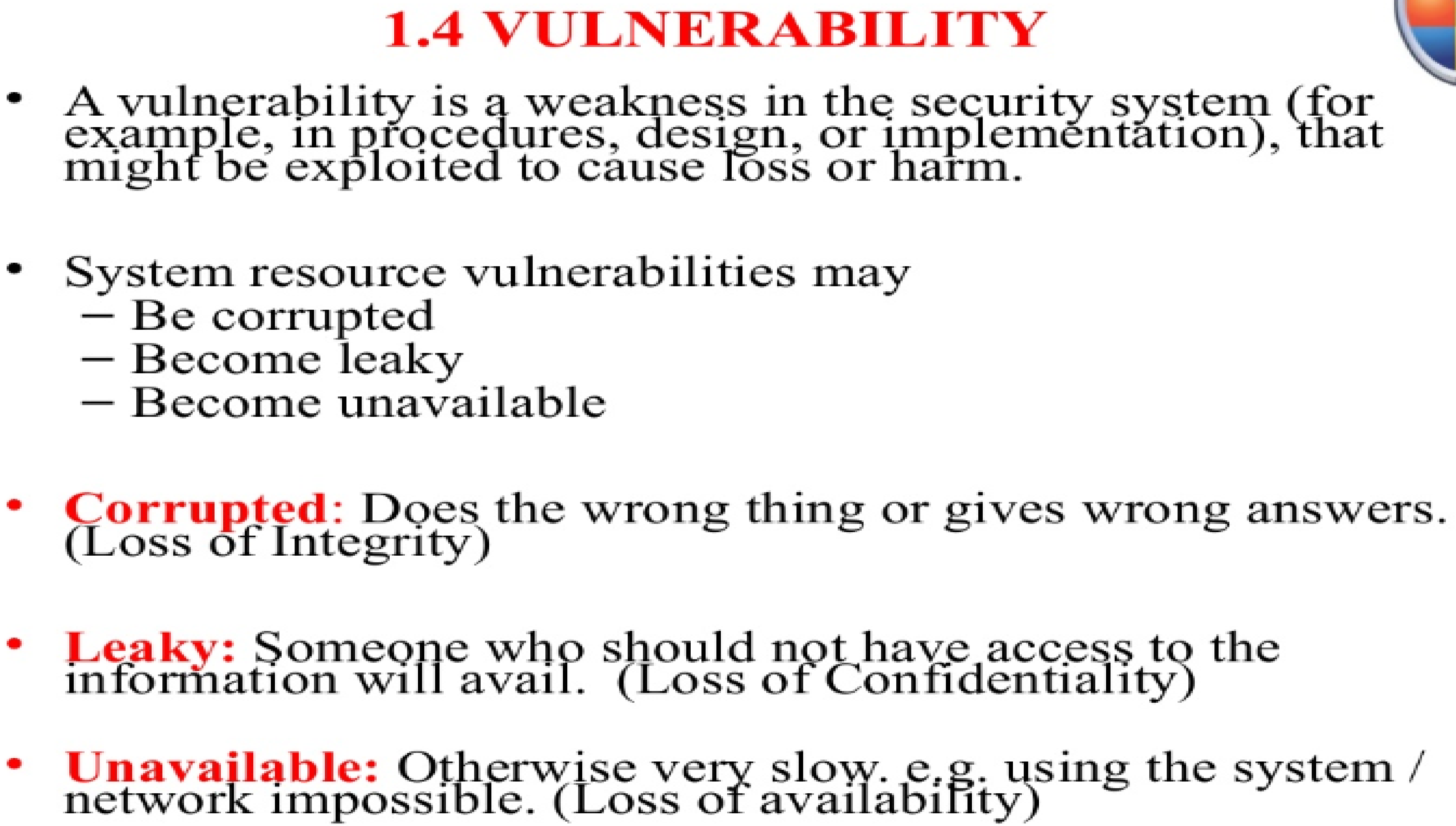
4. Risk - An expectation of loss expressed that a particular threat will exploit a particular vulnerability with a particular harmful result.



5. Security Policy - A set of rules and practices that specify how a system or an organization provides security services to protect sensitive and critical system resources.

6. Threat - A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

7. Vulnerability - Flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.



1.4 VULNERABILITY

- A vulnerability is a weakness in the security system (for example, in procedures, design, or implementation), that might be exploited to cause loss or harm.

- System resource vulnerabilities may
  - Be corrupted
  - Become leaky
  - Become unavailable

- **Corrupted:** Does the wrong thing or gives wrong answers. (Loss of Integrity)

- **Leaky:** Someone who should not have access to the information will avail. (Loss of Confidentiality)

- **Unavailable:** Otherwise very slow. e.g. using the system / network impossible. (Loss of availability)

1.4.1 TYPES OF VULNERABILITIES

- **Hardware Vulnerabilities**
  - adding devices, changing them, removing them, intercepting the traffic to them, or flooding them with traffic until they can no longer function. (many other ways to harm the hardware).

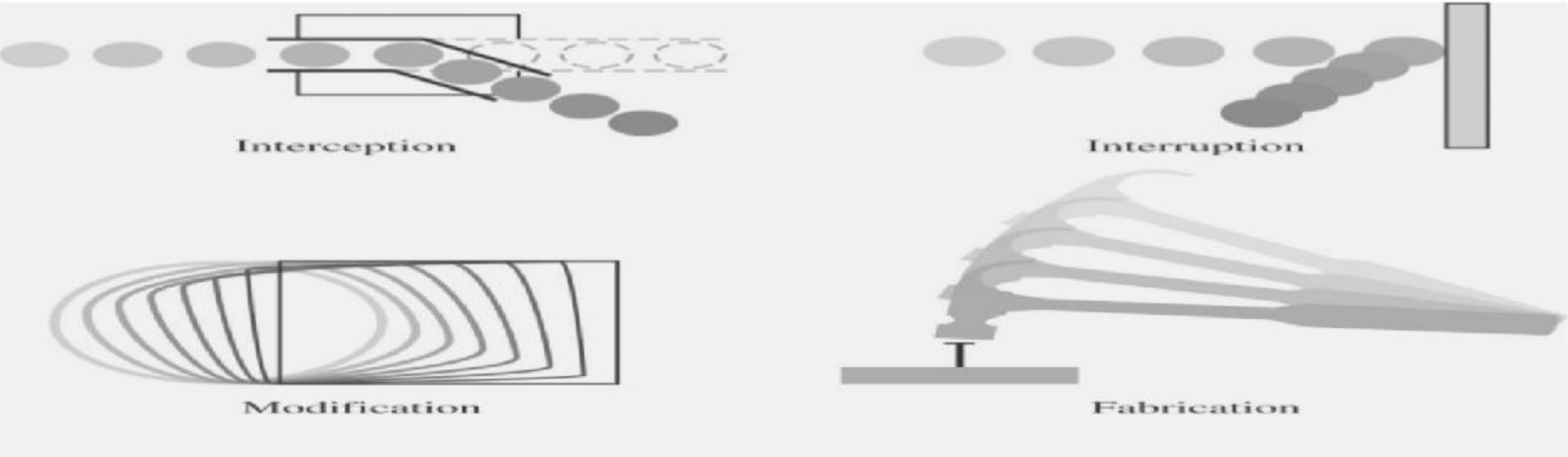
- **Software Vulnerabilities**
  - Software can be replaced, changed, or destroyed maliciously, or it can be modified, deleted, or misplaced accidentally. Whether intentional or not, these attacks exploit the software's vulnerabilities.

- **Data Vulnerabilities**
  - data have a definite value, even though that value is often difficult to measure.

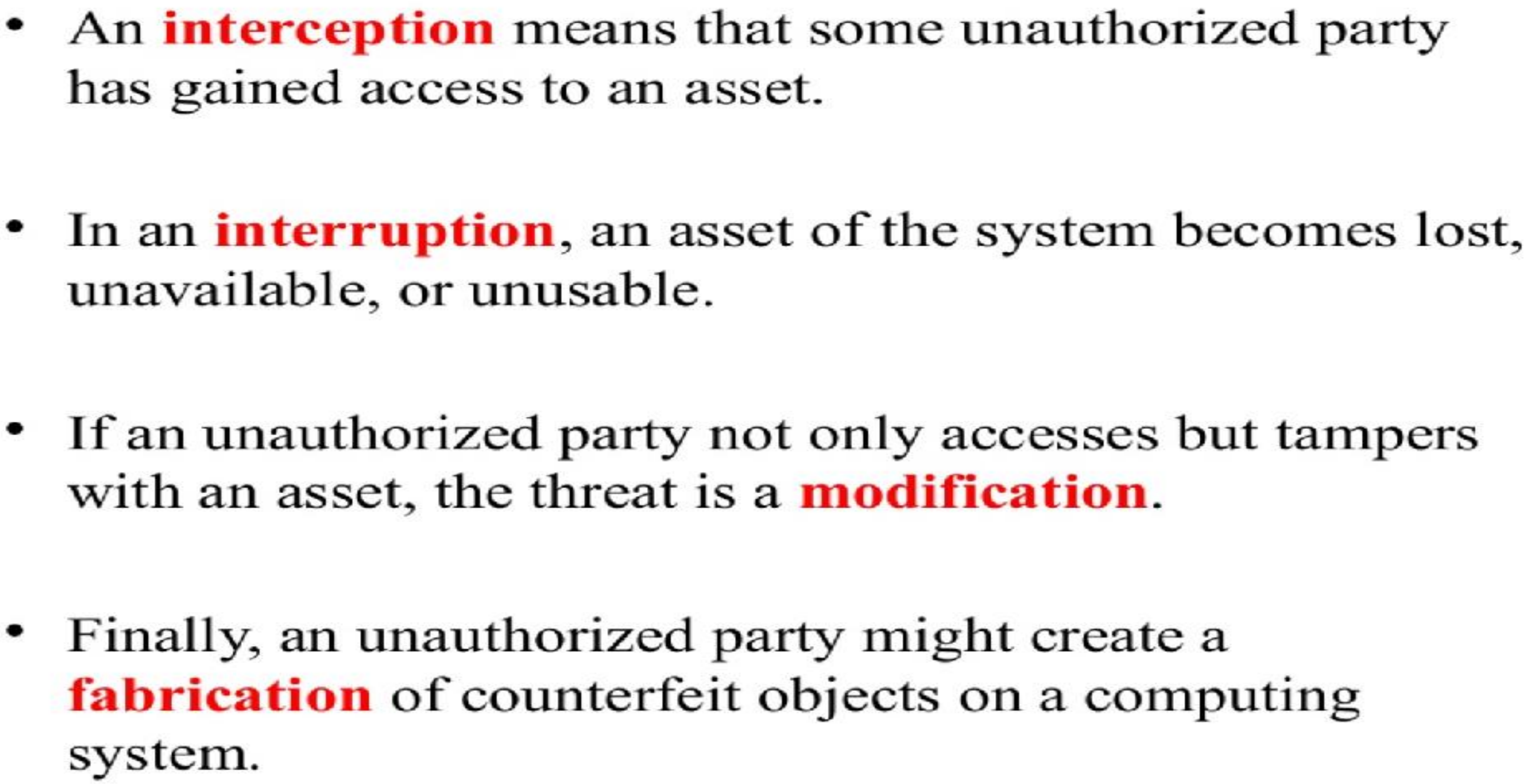
1.5 THREATS

- A **threat** to a computing system is a set of circumstances that has the potential to cause loss or harm.

- We can view any threat as being one of four kinds: interception, interruption, modification, and fabrication.



Pfleeger/Pfleeger Fig. 01-02



- An **interception** means that some unauthorized party has gained access to an asset.

- In an **interruption**, an asset of the system becomes lost, unavailable, or unusable.

- If an unauthorized party not only accesses but tampers with an asset, the threat is a **modification**.

- Finally, an unauthorized party might create a **fabrication** of counterfeit objects on a computing system.

1.6 ATTACKS

Attacks

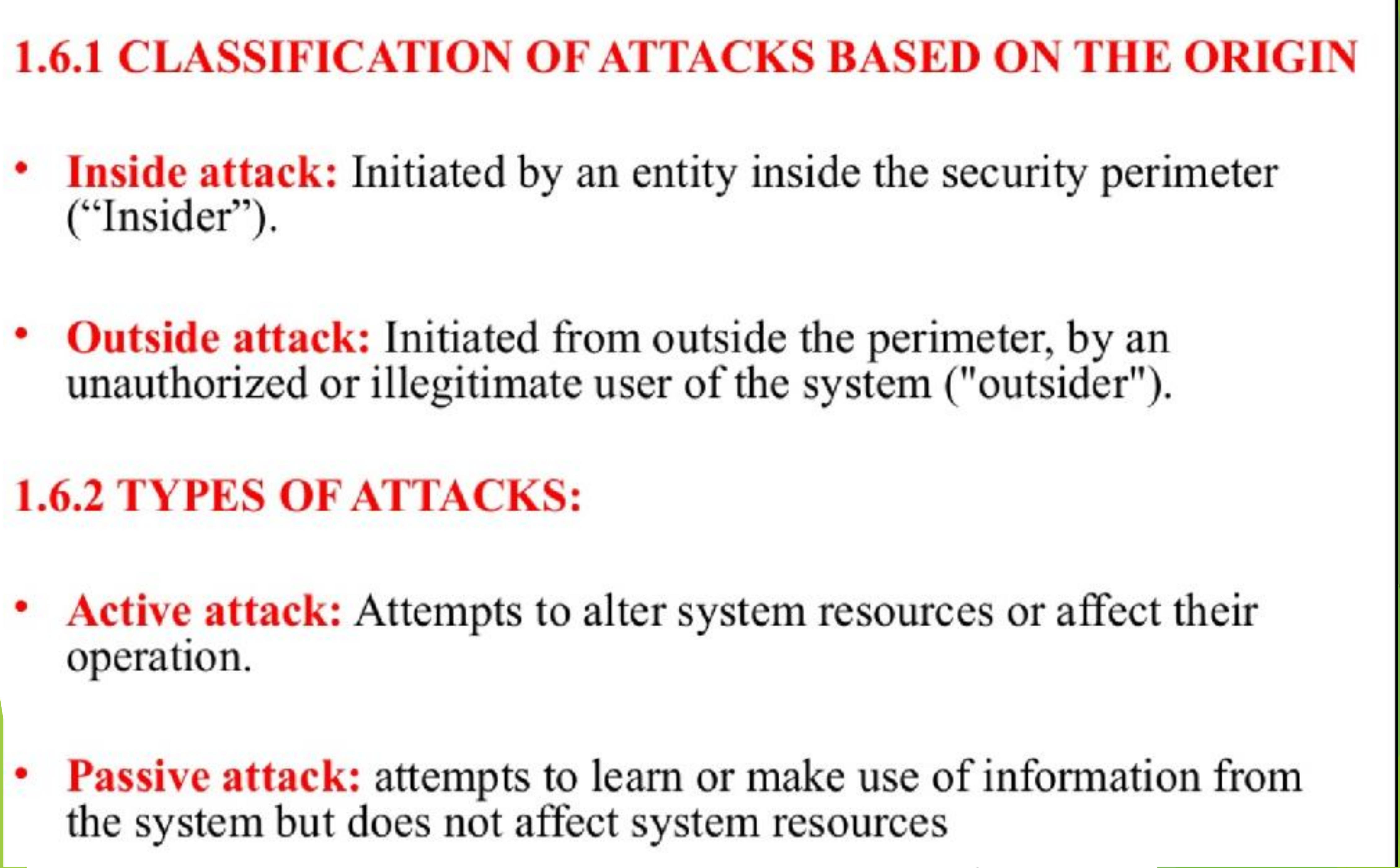
Attacks = Motive (Goal) + Method + Vulnerability

Motives

A motive originates out of the notion that the target system stores or processes something valuable and this leads to threat of an attack on the system

Attackers have motives or goals such as disrupting business continuity, information theft, data manipulations, or taking revenge

Goals



1.6.1 CLASSIFICATION OF ATTACKS BASED ON THE ORIGIN

- **Inside attack:** Initiated by an entity inside the security perimeter (“Insider”).

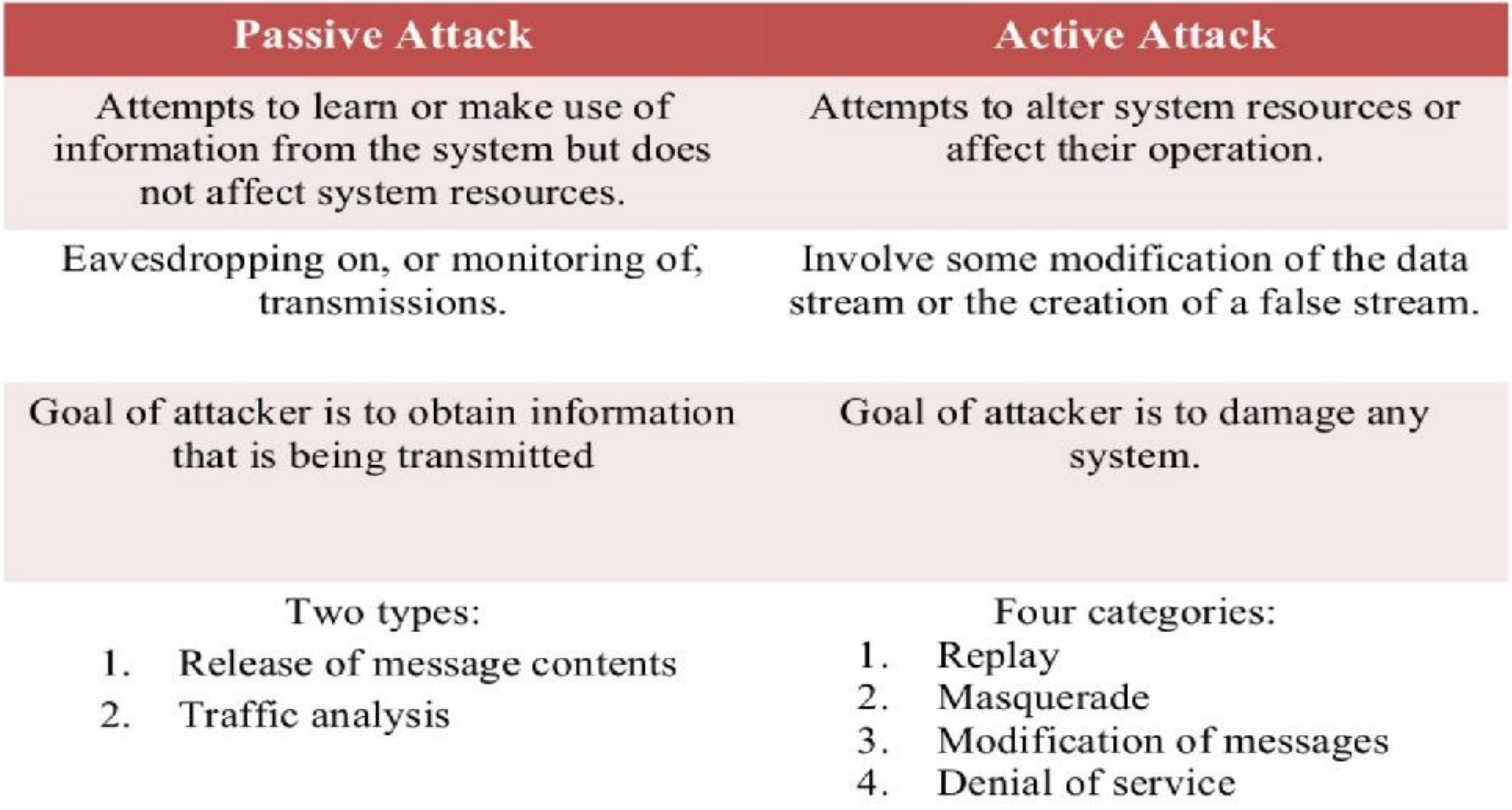
- **Outside attack:** Initiated from outside the perimeter, by an unauthorized or illegitimate user of the system ("outsider").

1.6.2 TYPES OF ATTACKS:

- **Active attack:** Attempts to alter system resources or affect their operation.

- **Passive attack:** attempts to learn or make use of information from the system but does not affect system resources

PASSIVE AND ACTIVE ATTACKS - DIFFERENCES



Passive Attack	Active Attack
Attempts to learn or make use of information from the system but does not affect system resources.	Attempts to alter system resources or affect their operation.
Eavesdropping on, or monitoring of, transmissions.	Involve some modification of the data stream or the creation of a false stream.
Goal of attacker is to obtain information that is being transmitted	Goal of attacker is to damage any system.
Two types: 1. Release of message contents 2. Traffic analysis	Four categories: 1. Replay 2. Masquerade 3. Modification of messages 4. Denial of service

1.7 ATTACK SURFACES

- Consist of the reachable and exploitable vulnerabilities in a system.

- Three types of attack surfaces

1. **Network Attack Surface** - Vulnerabilities over an enterprise network, wide-area network, or the Internet

2. **Software Attack Surface** - Vulnerabilities in application, utility, or operating system code

3. **Human Attack Surface** - Vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders.