

GLOBAL
EDITION

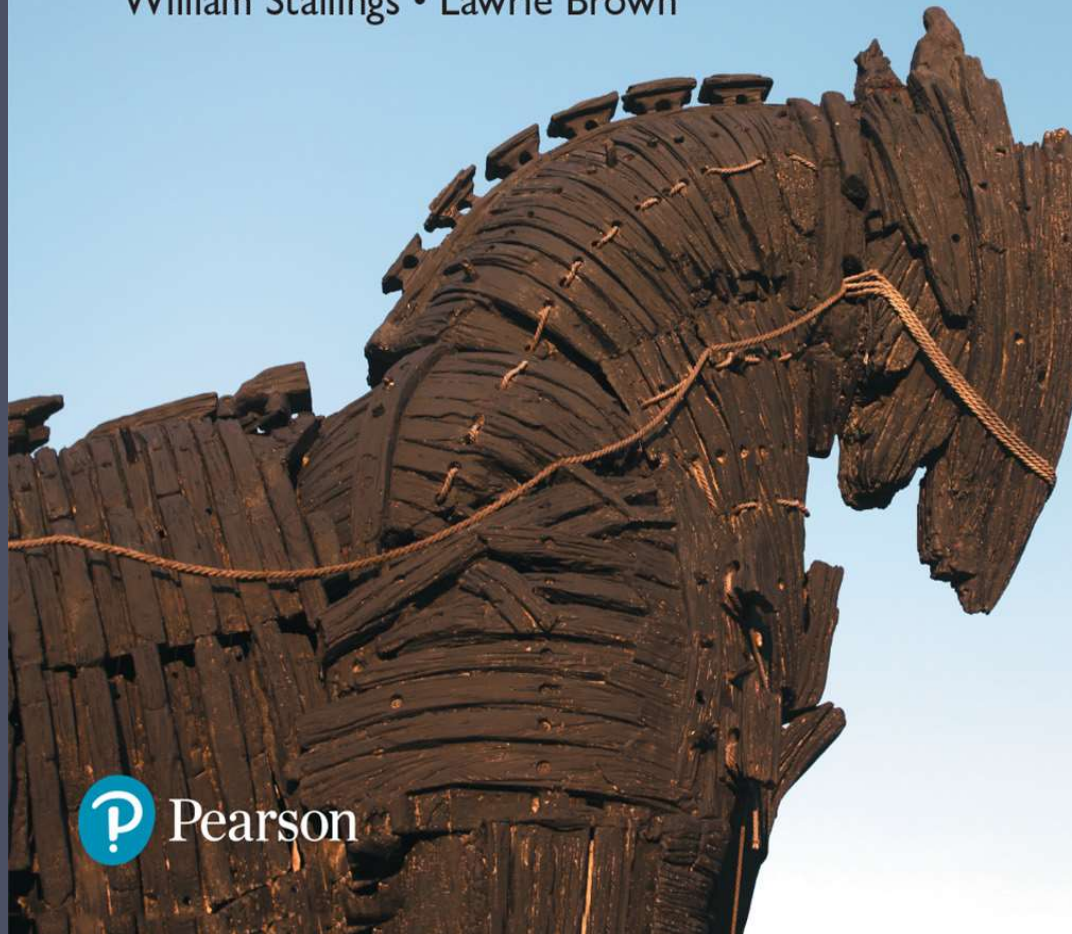


Computer Security

Principles and Practice

FOURTH EDITION

William Stallings • Lawrie Brown



Chapter 1

Overview

Computer Security

Computer Security is protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).



Key Security Concepts

The three key security concepts form what is often referred to as the **CIA triad**. The three concepts embody the fundamental security objectives for both data and for information and computing services.

السرية • **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

الصداقة • **Integrity:** Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

التوفر • **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

CIA Triad

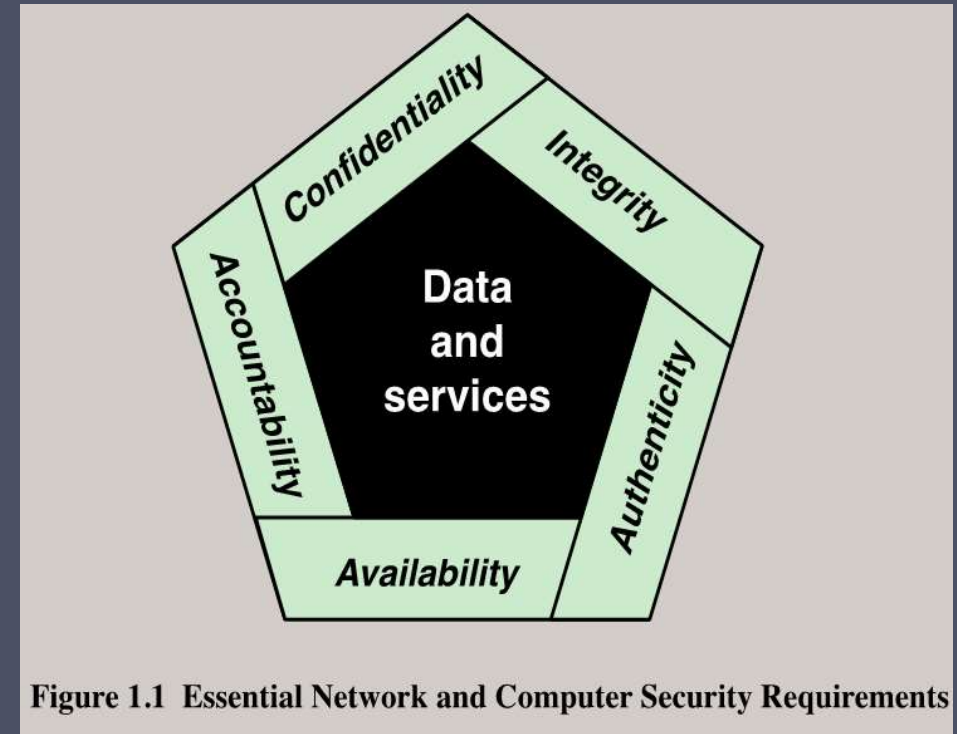
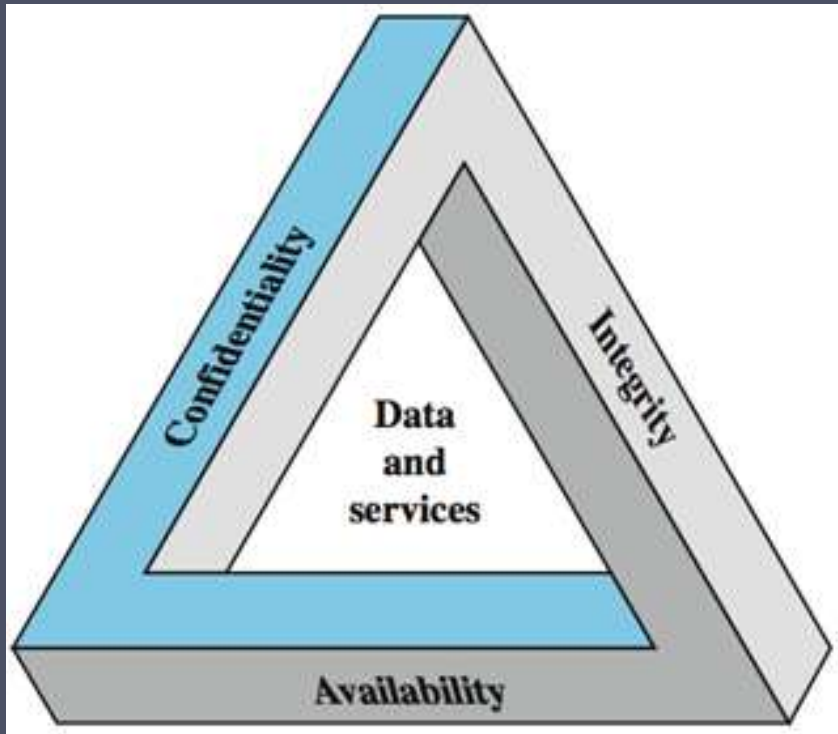


Figure 1.1 Essential Network and Computer Security Requirements

These three concepts form what is often referred to as the **CIA triad**. The **three concepts embody the fundamental security objectives for both data and for information and computing services**. Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture (see Figure 1.1).

Key Security Concepts

Confidentiality

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Integrity

- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity

Availability

- Ensuring timely and reliable access to and use of information

Additional Security concepts

Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture.

- **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.
- **Accountability**: The security goal that generates the **requirement for actions of an entity to be traced uniquely to that entity**.

ما ركز عليه الدكتور Computer Security Challenges

1. Computer security is not as simple as it might first appear to the novice
2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features
3. Procedures used to provide particular services are often counterintuitive
4. Physical and logical placement needs to be determined
5. Security mechanisms typically involve more than a particular algorithm or protocol and also require that participants be in possession of some secret information which raises questions about the creation, distribution, and protection of that secret information
6. Attackers only need to find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security
7. Security is still too often an afterthought to be incorporated into a system after the design is complete, rather than being an integral part of the design process
8. Security requires regular and constant monitoring
9. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs
10. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information

Computer Security Terminology

المخترق

تعريف

Adversary (threat agent)

Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Attack

الهجوم

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

Countermeasure

الدفاع

A device or techniques that has as its objective the impairment of the operational effectiveness of undesirable or adversarial activity, or the prevention of espionage, sabotage, theft, or unauthorized access to or use of sensitive information or information systems.

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.

Computer Security Terminology

Security Policy

سياسة الأمان

A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.

System Resource (Asset)

موارد

A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Figure 1.2 Security Concepts and Relationships

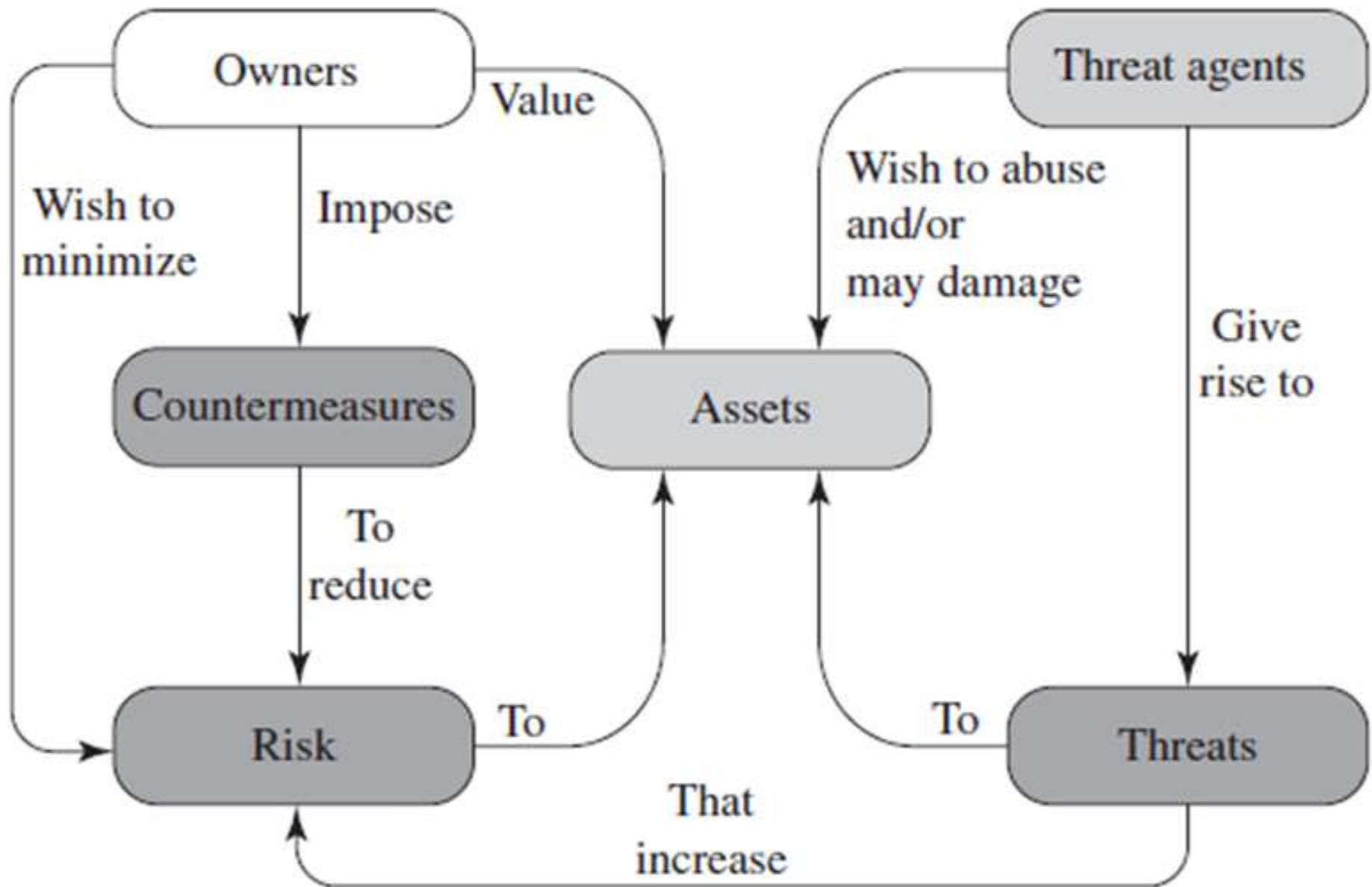


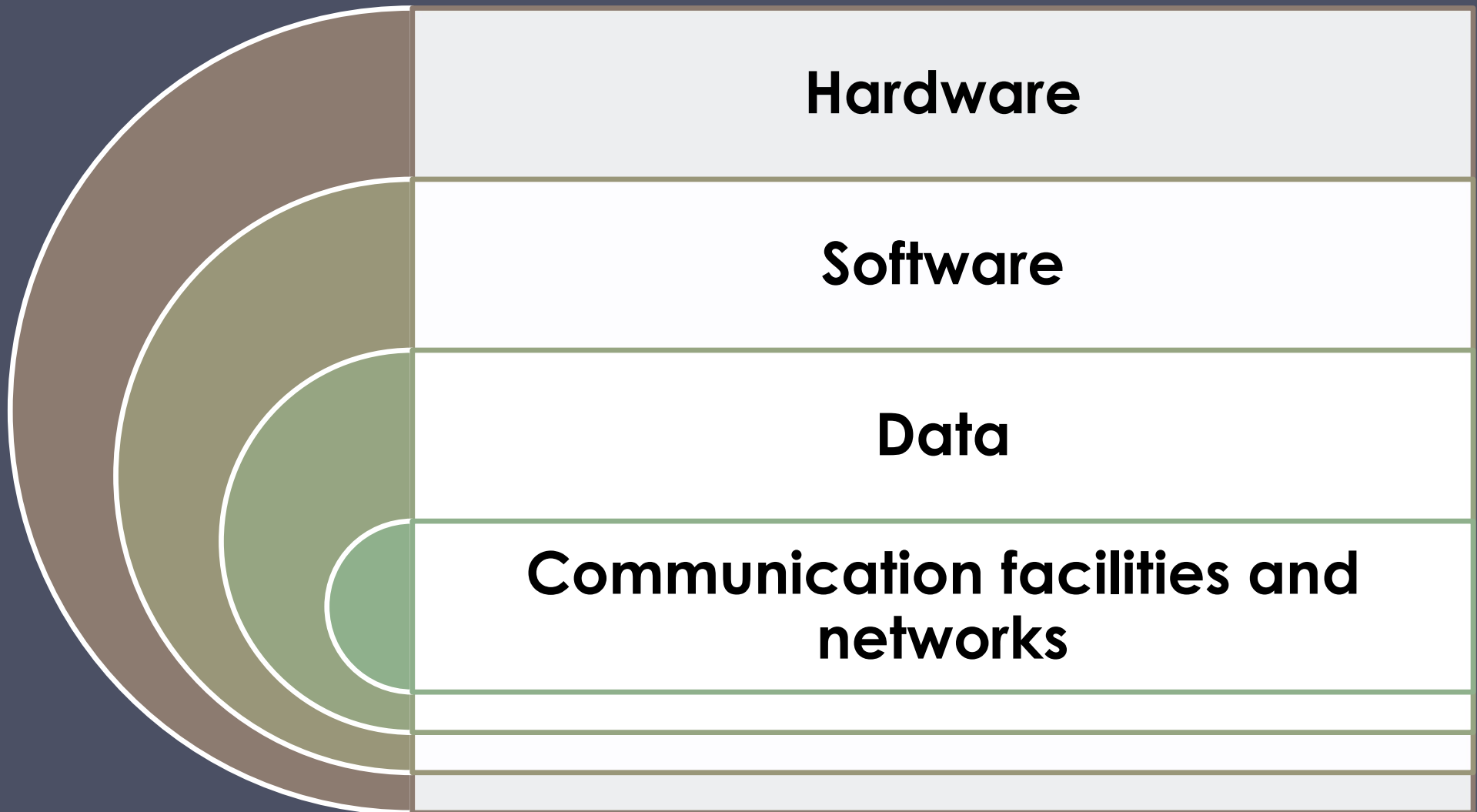
Figure Security Concepts and Relationships

Assets of a computer system


The assets of a computer system can be categorized as follows:

- **Hardware**: Including computer systems and other data processing, data storage, and data communications devices
- **Software**: Including the operating system, system utilities, and applications.
- **Data**: Including files and databases, as well as security-related data, such as password files.
- **Communication facilities and networks**: Local and wide area network communication links, bridges, routers, and so on.

✗ Assets of a Computer System



Vulnerabilities, Threats and Attacks

- Categories of vulnerabilities
 - Corrupted (loss of integrity)
 - Leaky (loss of confidentiality)
 - Unavailable or very slow (loss of availability)
- Threats 
 - Capable of exploiting vulnerabilities
 - Represent potential security harm to an asset
- Attacks (threats carried out)
 - Passive – attempt to learn or make use of information from the system that does not affect system resources
 - Active – attempt to alter system resources or affect their operation
 - Insider – initiated by an entity inside the security parameter
 - Outsider – initiated from outside the perimeter

Vulnerabilities

In the context of security, our concern is with the **vulnerabilities** of system resources. Following are general categories of vulnerabilities of a computer system or network asset:

- **Corrupted:** It can be **corrupted**, so that it does the wrong thing or gives wrong answers.
- **Leaky:** It can become **leaky**.
- **Unavailable:** It can become **unavailable** or very slow.

Type of Attacks

The agent carrying out the attack is referred to as an attacker, or **threat agent**. Based on **threat agent** We can distinguish two types of attacks:

- **Active attack:** An attempt to alter system resources or affect their operation.
- **Passive attack:** An attempt to learn or make use of information from the system that does not affect system resources.

We can also classify attacks based on the **origin of the attack:**

- 1 **Inside attack:** Initiated by an entity inside the security perimeter (an “insider”). The insider is authorized to access system resources but uses them in a way not approved by those who granted the authorization.
- 2 **Outside attack:** Initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an “outsider”). On the Internet, potential Outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

Countermeasures

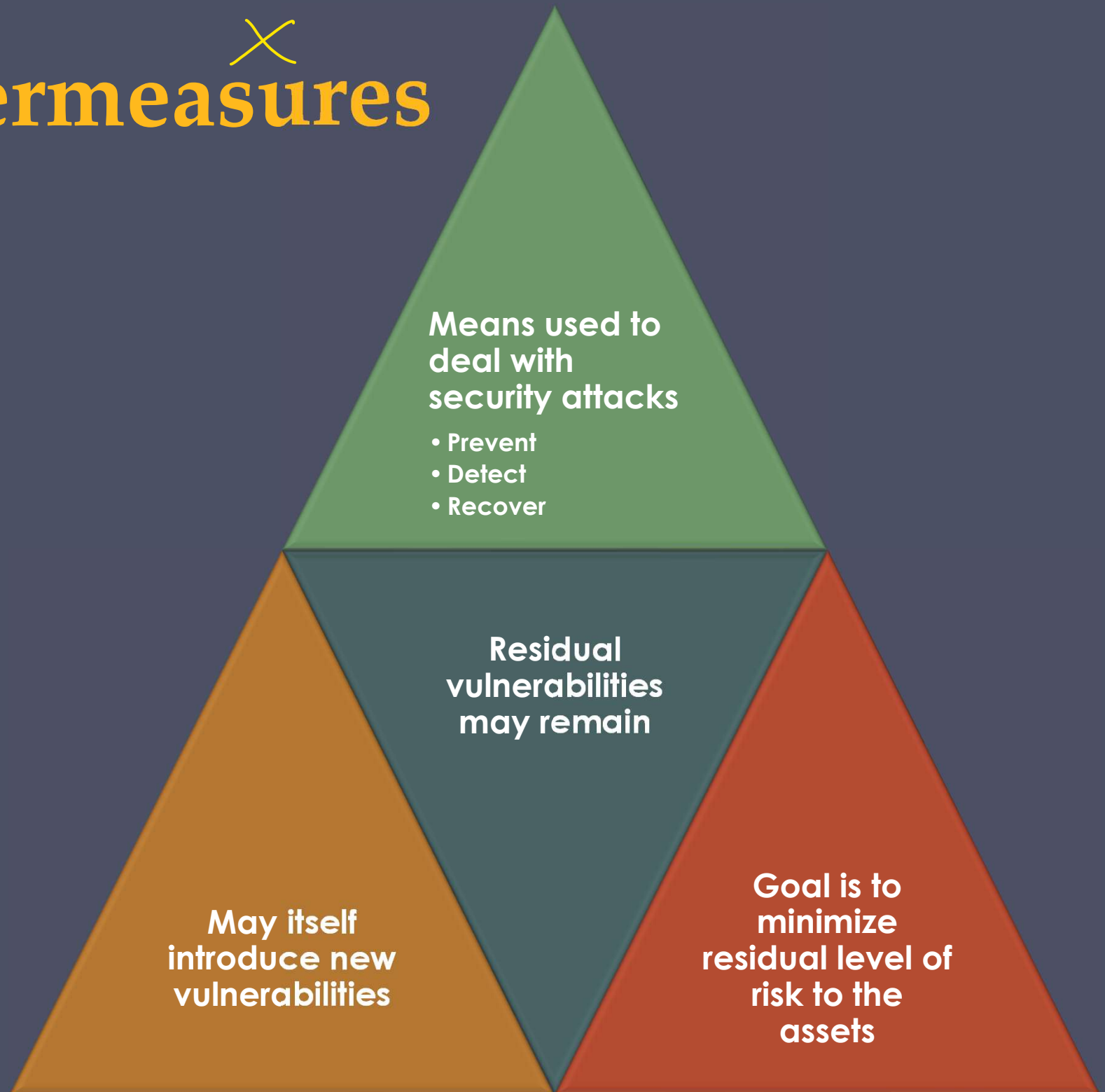
A countermeasure is **any means taken to deal with a security attack**. A countermeasure can be devised to

1 **prevent** a particular type of attack from succeeding.

When prevention is not possible, or fails in some instance, the goal is to² **detect** the attack and then

3 **recover** from the effects of the attack.

Countermeasures^x



Threat Consequences, and the Types of Threat

Actions that Cause Each Consequence

- unauthorized disclosure:
 - exposure, interception, inference, intrusion
- deception
 - masquerade, falsification, repudiation
- disruption
 - incapacitation, corruption, obstruction
- usurpation
 - misappropriation, misuse

Unauthorized Disclosure

Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure: A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	Exposure: Sensitive data are directly released to an unauthorized entity. Interception: An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. Inference: A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or by-products of communications. Intrusion: An unauthorized entity gains access to sensitive data by circumventing a system's security protections.

Deception

Threat Consequence	Threat Action (Attack)
Deception: A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	Masquerade: An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. Falsification: False data deceive an authorized entity. Repudiation: An entity deceives another by falsely denying responsibility for an act.

Disruption

Threat Consequence	Threat Action (Attack)
Disruption: A circumstance or event that interrupts or prevents the correct operation of system services and functions.	Incapacitation: Prevents or interrupts system operation by disabling a system component. Corruption: Undesirably alters system operation by adversely modifying system functions or data. Obstruction: A threat action that interrupts delivery of system services by hindering system operation.

Usurpation

Threat Consequence	Threat Action (Attack)
Usurpation: A circumstance or event that results in control of system services or functions by an unauthorized entity.	Misappropriation: An entity assumes unauthorized logical or physical control of a system resource. Misuse: Causes a system component to perform a function or service that is detrimental to system security.

Table 1.3

Computer and Network Assets, with Examples of Threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Network Security Attacks

Network security attacks can be classified as *passive attacks* and *active attacks*.

A **passive attack** attempts to learn or make use of information from the system but does not affect system resources.

An **active attack** attempts to alter system resources or affect their operation.

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the attacker is to obtain information that is being transmitted.

Types of passive attacks

Two types of passive attacks are the release of message contents and traffic analysis.

- The **release of message contents** is easily understood. A **telephone conversation**, an **electronic mail** message, and a transferred file may contain sensitive or confidential information.
- A second type of passive attack, **traffic analysis**, is subtler. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message.

Types of Active attacks

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: replay, masquerade, modification of messages, and denial of service.

- **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- A **masquerade** takes place when one entity pretends to be a different entity.
- **Modification of messages** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. DDoS
- The **denial of service** prevents or inhibits the normal use or management of communication facilities.

Thank You!