Introduction to Security

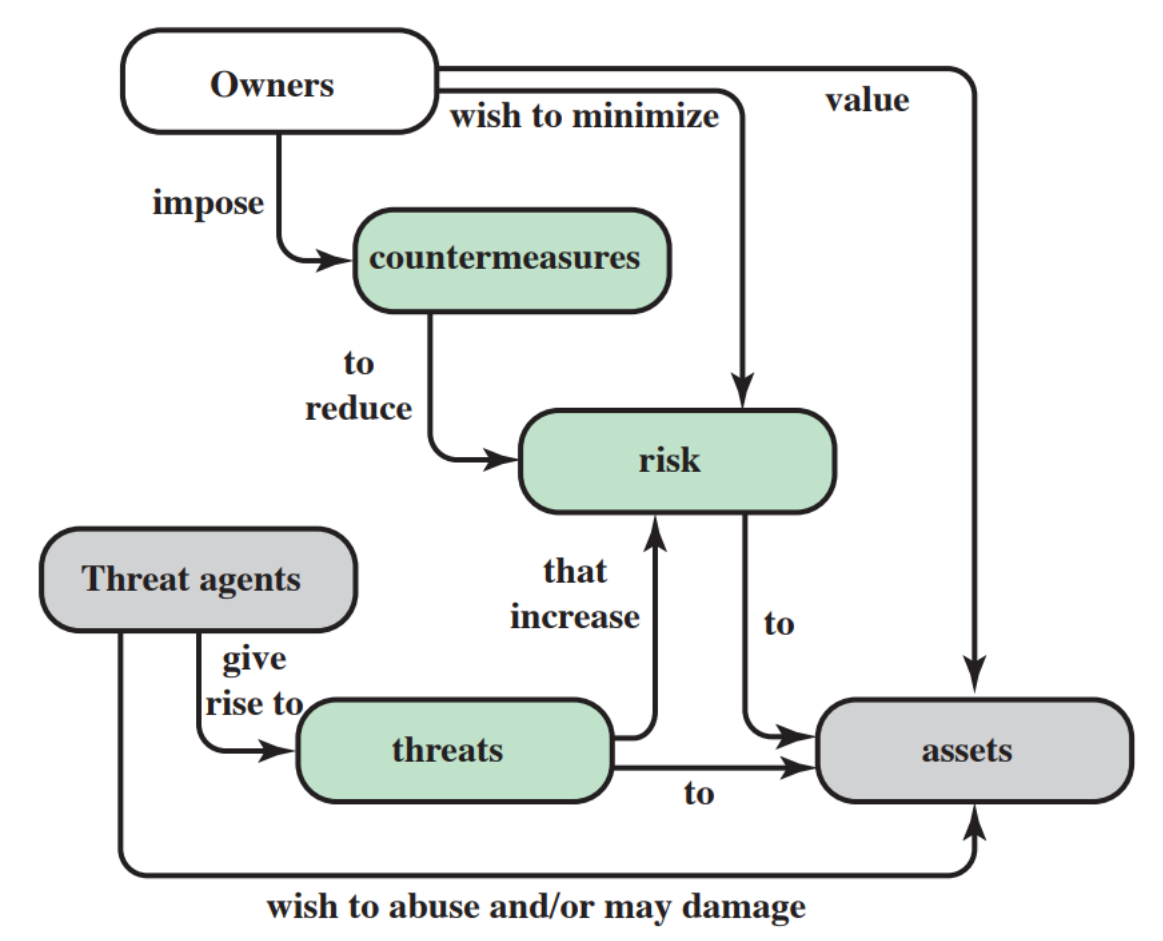
COMPUTER SCIENCE DEPARTMENT

COMP438

Dr. Abdallah Karakra

Wednesday, October 2, 2024

Security Concepts and Relationship



Computer Security: Principles and Practice, 3rd Edition
William Stallings
Lawrie Brown

What is computer security?

- The NIST Computer Security Handbook [NIST95] defines the term computer security as follows:

> **Computer Security**: The 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).

The National Institute of Standards and Technology Framework (NIST)

Computer Security Objectives (CIA triad)

Confidentiality

- Data confidentiality
  - Assures that private or confidential information **is not** made available or disclosed to unauthorized individuals.
- Privacy
  - Assures that **individuals control** or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Computer Security Objectives

Integrity

- Data integrity
  - Assures that information and programs are changed only in a specified and authorized manner.
- System integrity
  - Assures that a system performs its intended function in an unimpaired manner , free from deliberate or inadvertent unauthorized manipulation of the system.

Availability

- Assures that systems work promptly and service is not denied to authorized users.

Breach of Security Levels of Impact

- **High**
  - The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals
- **Moderate**
  - The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals
- **Low**
  - The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals
    Example: minor financial loss

Computer Security Challenges

- Security is not simple.
- Potential attacks on the security features need to be considered.
- Procedures used to provide particular services are often counter-intuitive.
- It is necessary to decide where to use the various security mechanisms.
- Requires constant monitoring.
- Is too often an afterthought.

- Security mechanisms typically involve more than a particular algorithm or protocol.
- Security is essentially a battle of wits between a perpetrator and the designer.
- Little benefit from security investment is perceived until a security failure occurs.
- Strong security is often viewed as an impediment to efficient and user-friendly operation.

Computer Security Terminology

- **Adversary**
- **Attack**
- **Countermeasure**
- **Security Policy**
- **System Resource (Asset)**
- **Vulnerability**
- **Threat**
- **Risk**

Threat, Vulnerability, & risk

Man

Open Window

Mosquito

Risk

Vulnerability

Threat

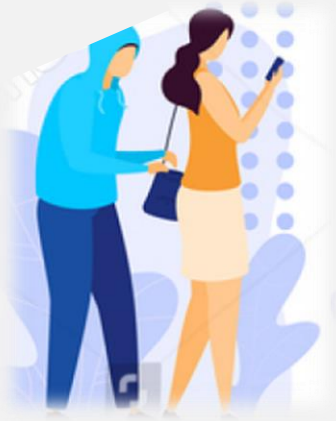
when the Mosquito bite the man

Example: protect a home

Threat

Risk

Vulnerability



???

Computer Security Terminology

Adversary (threat agent)
Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

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

Countermeasure
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.

Security Policy
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)
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.

Source: Stallings, William, Computer Security: Principles and Practice, 4e., ©2019. Reprinted and electronically reproduced by permission of pearson education, inc., new york, ny.

Basic Attacker Model

- The basic attacker model is a framework for understanding the various types of attackers and the threats they pose. In other words, the attacker model allows for an understanding of the capabilities and motivations of an adversary, as well as the target system they aim to exploit. It is used to identify the different ways that an attacker can exploit a system's vulnerabilities and achieve their goals. Additionally, it can be used to develop strategies for defending against cyberattacks.

- By understanding the attacker's capabilities and motivations, organizations can better defend themselves against potential attacks.

Basic Attacker Model

- What type of action will they take?
  - Passive (look, but don't touch)
  - Active (look and inject messages)
- How sophisticated are they?
  - Ranges from script kiddies to government-funded group of professionals
- How much do they already know?
  - External attacker: no knowledge of cryptographic information, no access to resources
  - Internal attacker: complete knowledge of all cryptographic information, complete access Result of system compromise

Attackers with minimal skills and knowledge who use pre-written scripts and tools to carry out attacks.

Attackers with a high level of skill and resources who are often responsible for the most sophisticated and damaging attacks.