Computer Security: Principles and Practice

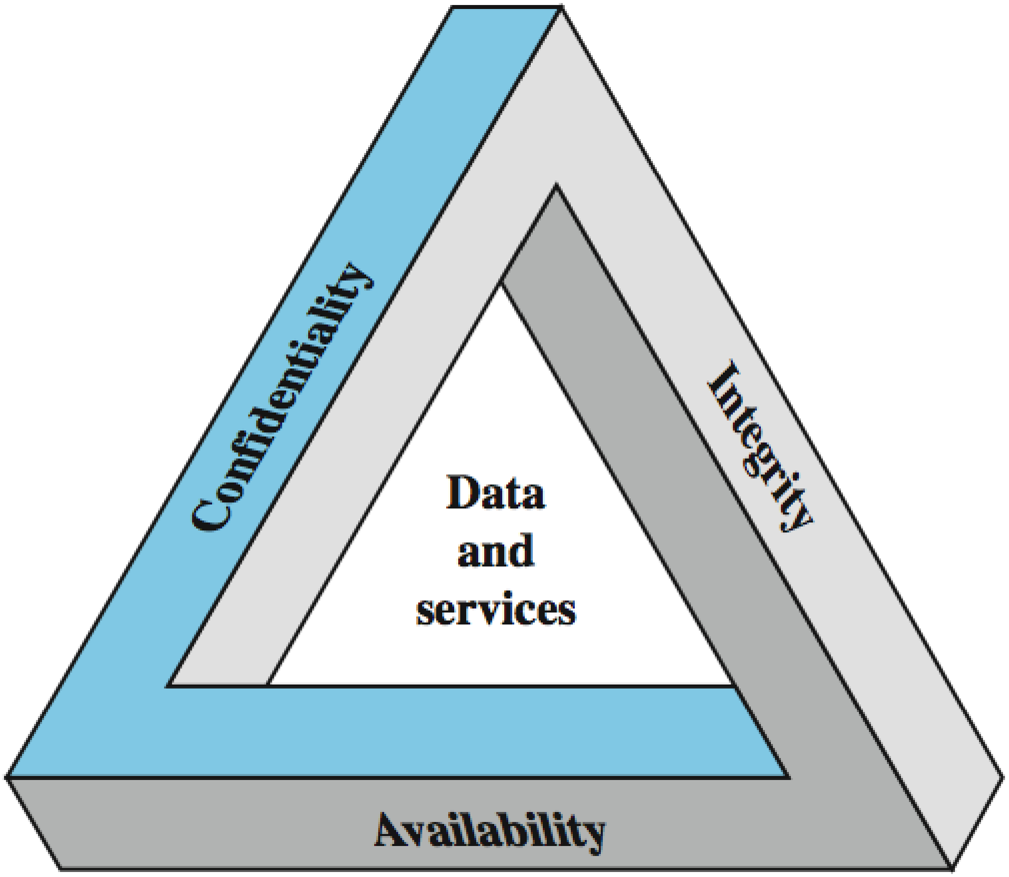
Overview

Overview

Computer Security:

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



CIA Triad

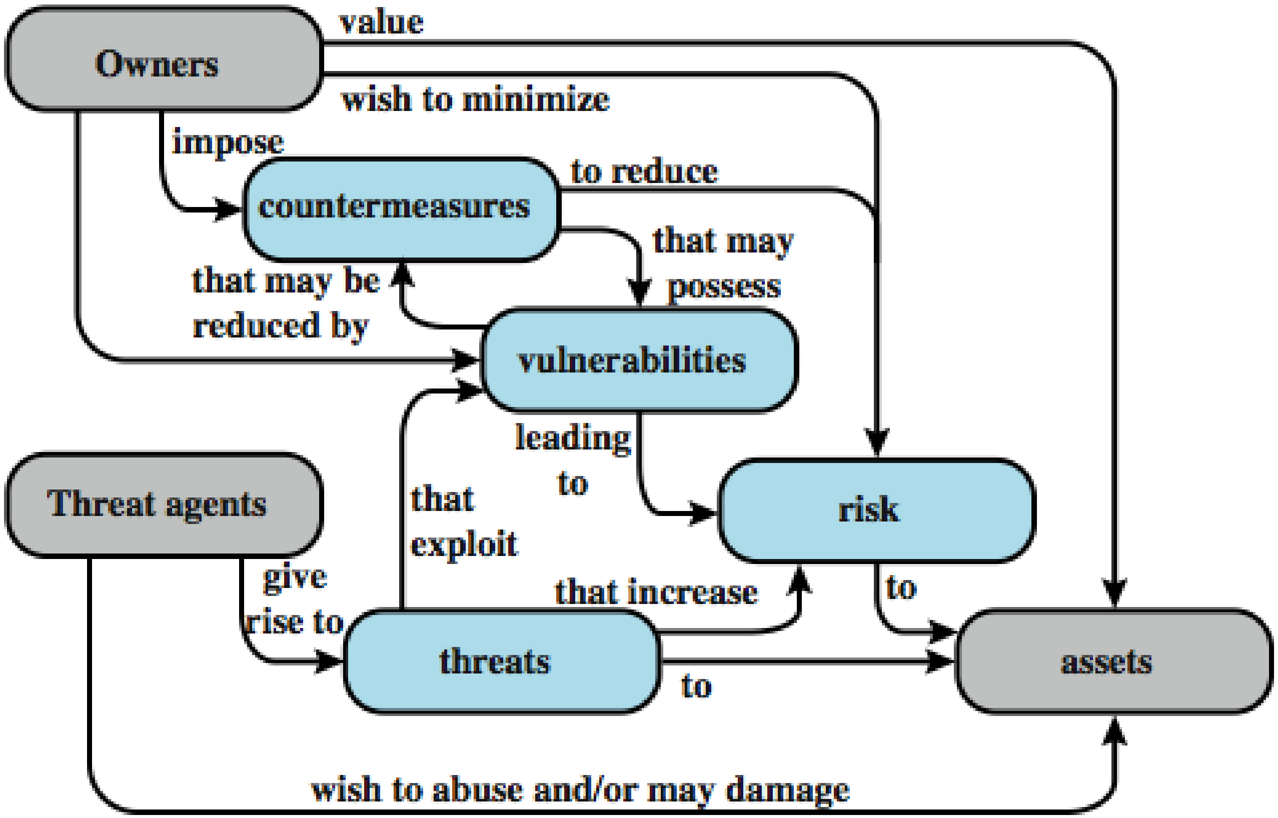
- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
  - *Data confidentiality*
  - *Privacy*
  - A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity:** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
  - *Data integrity*
  - *System integrity*
  - A loss of integrity is the unauthorized modification or destruction of information.
- **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.

- **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.

Computer Security Challenges

1. not simple
2. must consider potential attacks
3. procedures used counter-intuitive
4. involve algorithms and secret info
5. must decide where to deploy mechanisms
6. battle of wits between attacker / admin
7. not perceived on benefit until fails
8. requires regular monitoring
9. too often an after-thought
10. regarded as impediment to using system

Security Terminology



Security Terminology

- **Adversary (threat agent)** - An entity that attacks, or is a threat to, a system.
- **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.
- **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, or by discovering and reporting it so that corrective action can be taken.
- **Risk** - An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
- **Security Policy** - A set of rules and practices that specify how a system or org provides security services to protect sensitive and critical system resources.

Security Terminology

- **System Resource (Asset)** –
  - Data;
  - a service provided by a system;
  - a system capability;
  - an item of system equipment;
  - a facility that houses system operations and equipment.
- **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.
- **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.

Vulnerabilities and Attacks

- system resource vulnerabilities may
  - be corrupted (loss of integrity)
  - become leaky (loss of confidentiality)
  - become unavailable (loss of availability)
- attacks are threats carried out and may be
  - **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
- We can also classify attacks based on the origin of the attack:
  - **Inside attack:** Initiated by an entity inside the security perimeter (an "insider)
  - **Outside attack:** Initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider").

Countermeasures

- means used to deal with security attacks
  - prevent
  - detect
  - recover
- may result in new vulnerabilities
- will have residual vulnerability
- goal is to minimize risk given constraints

Threat Consequences

- Unauthorized disclosure
    - exposure, interception, inference, intrusion
- Deception
    - masquerade, falsification, repudiation
- Disruption
    - incapacitation, corruption, obstruction
- Usurpation
    - misappropriation, misuse

Unauthorized disclosure

- **Exposure:** Sensitive data is directly released to an unauthorized entity.
- **Interception:** An unauthorized entity directly accesses sensitive data in transit.
- **Inference:** an unauthorized entity indirectly accesses sensitive data by reasoning from characteristics or by-products of communications.
- **Intrusion:** An unauthorized entity circumvents system's security protections.

Deception

- a threat to either system integrity or data integrity:
    - **Masquerade:** An unauthorized entity poses as an authorized entity.
    - **Falsification:** False data deceives an authorized entity.
    - **Repudiation:** An entity deceives another by falsely denying responsibility for an act.

Disruption

- a threat to availability or system integrity:
  - **Incapacitation:** Prevent/interrupt system operation by disabling a system component
  - **Corruption:** adversely modifying system functions or data
  - **Obstruction:** interrupts delivery of system services by hindering system operation.

Usurpation

- is a threat to system integrity:
  - **Misappropriation:** unauthorized logical or physical control of a system resource.
  - **Misuse:** Causes system to perform a function or service detrimental to security.

Threat & assets

- **Hardware -** A major threat is the threat to availability. Hardware is the most vulnerable to attack and the least susceptible to automated controls. Threats include accidental and deliberate damage to equipment as well as theft.
- **Software -** includes the operating system, utilities, and application programs. A key threat is an attack on availability. Software is often easy to delete. Software can also be altered or damaged to render it useless.

Threat & assets

- **Data –**
  - involves files and other forms of data controlled by individuals, groups, and business organizations.
  - Security concerns with respect to data are broad, encompassing availability, secrecy, and integrity.
  - In the case of availability, the concern is with the destruction of data files, which can occur either accidentally or maliciously.
  - The obvious concern with secrecy is the unauthorized reading of data files or databases.
  - A less obvious secrecy threat involves the analysis of data and manifests itself in the use of so-called statistical databases, which provide summary or aggregate information.
  - Finally, data integrity is a major concern in most installations.
  - Modifications to data files can have consequences ranging from minor to disastrous.

Network Security Attacks

- classify as passive or active
- passive attacks are eavesdropping
  - release of message contents
  - traffic analysis
  - are hard to detect so aim to prevent
- active attacks modify/fake data
  - masquerade
  - replay
  - modification
  - denial of service
  - hard to prevent so aim to detect

Cryptography

- Cryptography or “secret codes” are a fundamental information security tool
- has many uses, including the protection of confidentiality and integrity, among many other vital information security functions
- Modern cryptography
  - Symmetric-key cryptography
  - Public-key cryptography
  - Cryptanalysis
  - Cryptographic primitives
  - Cryptosystems

Access Control

- Access control deals with authentication and authorization
- Authentication
  - Passwords
  - biometrics and smartcards.
- Authorization deals with restrictions placed on authenticated users

Protocols

- an abstract or concrete protocol that performs a security-related function and applies cryptographic methods, often as sequences of cryptographic primitives.
- A protocol describes how the algorithms should be used

Computer Security Strategy

- specification/policy
  - what is the security scheme supposed to do?
  - codify in policy and procedures
- implementation/mechanisms
  - how does it do it?
  - prevention, detection, response, recovery
- correctness/assurance
  - does it really work?
  - assurance, evaluation

Summary

- security concepts
- terminology
- security strategy
- functional requirements