Chap 1: Overview

Outline

The focus of this chapter is on three fundamental questions:

- What assets do we need to protect?
- How are those assets threatened?
- What can we do to counter those threats?

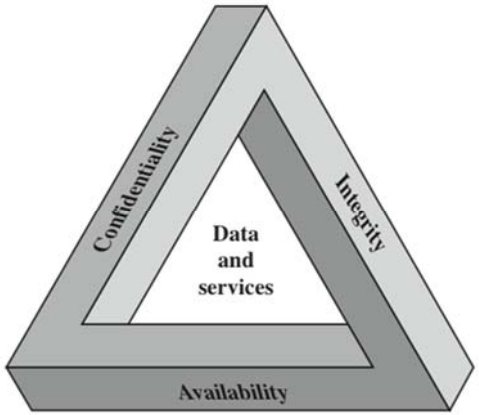
Computer Security Overview

- The NIST Computer Security Handbook defines the term **Computer Security** as:

  "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 CIA Triad



security requirement triad

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

Is this all?

Levels of Impact

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

Computer Security Challenges

- computer security is not as simple as it might first appear to the novice
- potential attacks on the security features must be considered
- procedures used to provide particular services are often counterintuitive
- physical and logical placement needs to be determined
- multiple algorithms or protocols may be involved

Computer Security Challenges

- attackers only need to find a **single** weakness, the developer needs to find **all** weaknesses
- users and system managers tend to not see the benefits of security until a failure occurs
- security requires regular and constant monitoring
- is often an afterthought to be incorporated into a system after the design is complete
- thought of as an impediment to efficient and user-friendly operation

Computer 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.

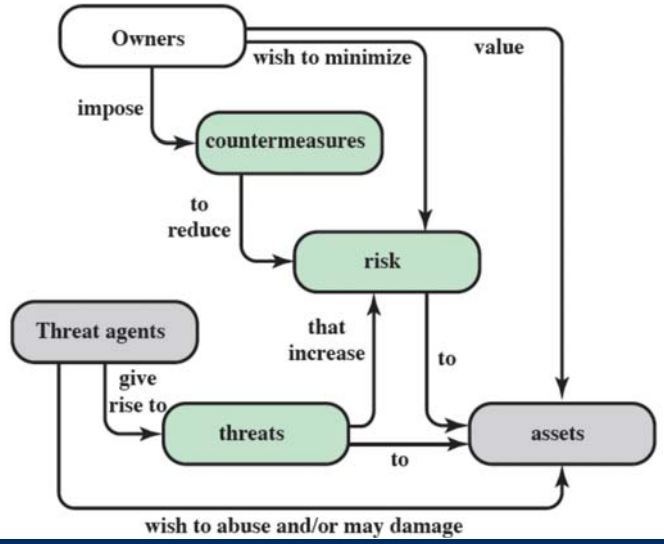
Computer Security Terminology

- **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.
- **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.

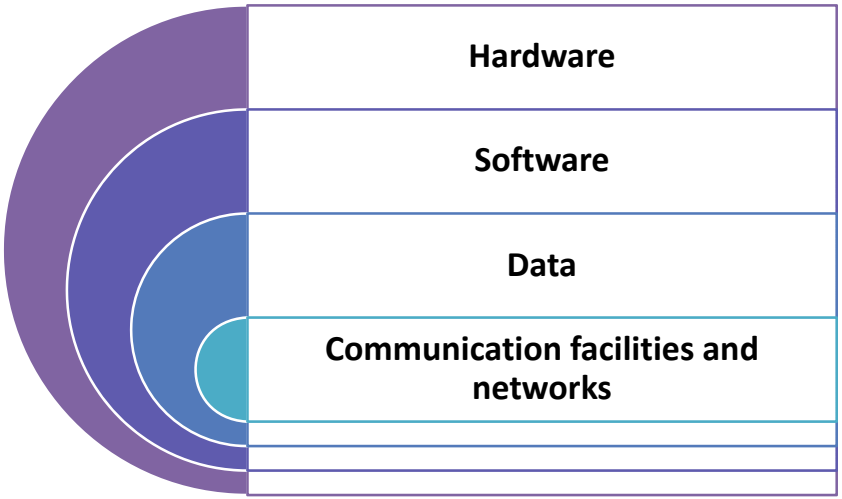
Computer Security Terminology

- **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.

Security Concepts and Relationships



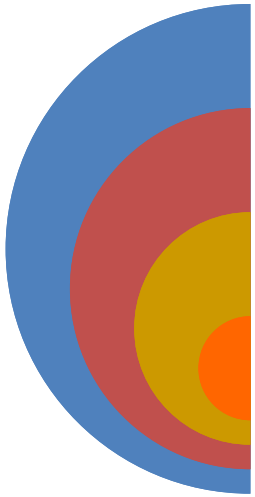
Assets of a Computer System



Vulnerabilities, Threats and Attacks

- vulnerabilities
  - leaky (loss of confidentiality)
  - corrupted (loss of integrity)
  - unavailable or very slow (loss of availability)
- threats
  - capable of exploiting vulnerabilities
  - represent potential security harm
- attacks (threats carried out)
  - passive or active attempt to alter/affect system resources
  - insider or outsider

Countermeasures



means used to deal with security attacks

- **prevent**
- **detect**
- **recover**

may introduce new vulnerabilities

Residual vulnerabilities may remain

goal is to minimize residual level of risk to the assets

by Peter Steiner,
New York, July 5, 1993

"On the Internet, nobody knows you're a dog."

Threat Consequences

Unauthorized disclosure is a threat to *confidentiality*

- ***Exposure***: This can be deliberate or be the result of a human, hardware, or software error
- ***Interception***: unauthorized access to data (communication)
- ***Interference***: e.g., traffic analysis or use of limited access to get detailed information
- ***Intrusion***: unauthorized access to sensitive data (system)

Threat Consequences

Deception is a threat to either system or data *integrity*

- ***Masquerade***: an attempt by an unauthorized user to gain access to a system by posing as an authorized user
- ***Falsification***: altering or replacing of valid data or the introduction of false data
- ***Repudiation***: denial of sending, receiving or possessing the data.

Threat Consequences

Usurpation is a threat to system *integrity*.

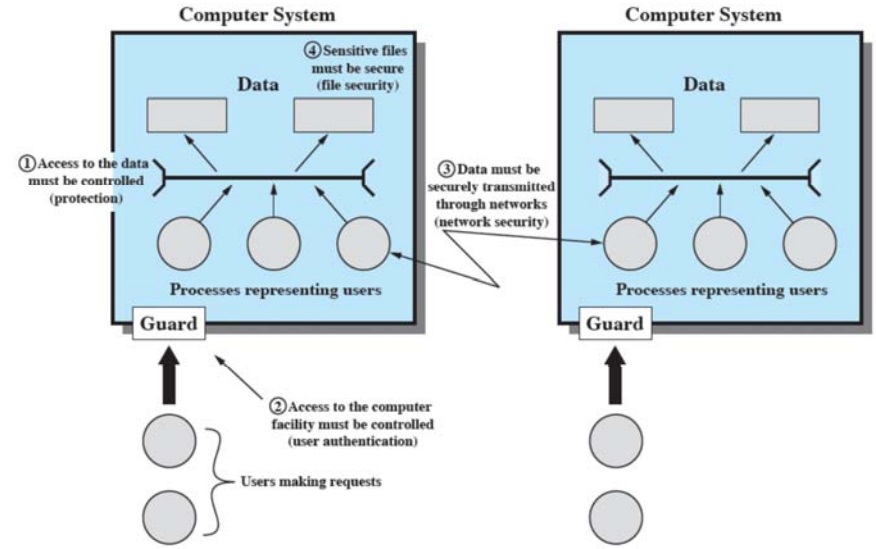
- ***Misappropriation***: e.g., theft of service, distributed denial of service attack
- ***Misuse***: security functions can be disabled or thwarted

Threat Consequences

Disruption is a threat to *availability* or system *integrity*

- ***Incapacitation***: a result of physical destruction of or damage to system hardware
- ***Corruption***: system resources or services function in an unintended manner; unauthorized modification
- ***Obstruction***: e.g. overload the system or interfere with communications

Scope of Computer Security



Computer and Network Assets w/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.

Passive and Active Attacks

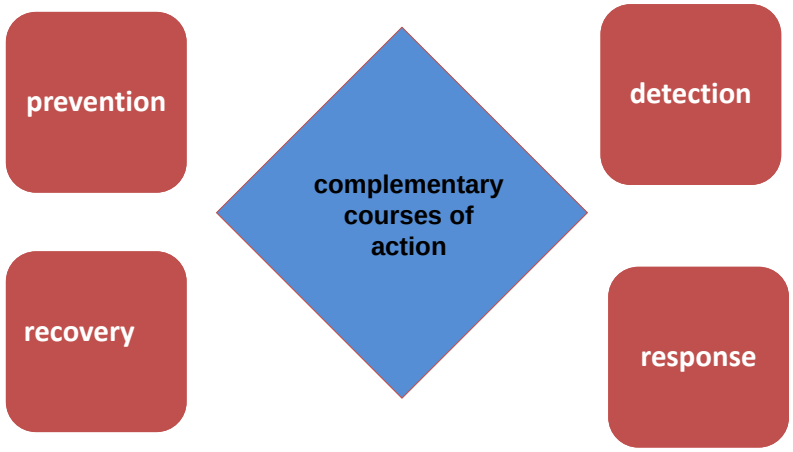
- **Passive attacks** attempt to learn or make use of information from the system but does not affect system resources
  - eavesdropping/monitoring transmissions
  - difficult to detect
  - emphasis is on prevention rather than detection
  - two types:
    - release of message contents
    - traffic analysis

- **Active attacks** involve modification of the data stream
  - goal is to detect them and then recover
  - categories:
    - masquerade
    - replay
    - modification of messages
    - denial of service

Security Functional Requirements

computer security technical measures	management controls and procedures	overlap computer security technical measures and management controls
• access control • identification & authentication; • system & communication protection • system & information integrity	• awareness & training • audit & accountability • certification, accreditation, & security assessments • contingency planning • maintenance • physical & environmental protection • planning • personnel security • risk assessment • systems & services acquisition	• configuration management • incident response • media protection

Security Implementation



Security Mechanism

- Feature designed to
  - Prevent attackers from violating security policy
  - Detect attackers' violation of security policy
  - Response to mitigate attack
  - Recover, continue to function correctly even if attack succeeds
- No single mechanism that will support all services
  - Authentication, authorization, availability, confidentiality, integrity, non-repudiation

Fundamental Security Design Principles

Economy of mechanism	Fail-safe defaults	Complete mediation	Open design
Separation of privilege	Least privilege	Least common mechanism	Psychological acceptability
Isolation	Encapsulation	Modularity	Layering
Least astonishment			

Attack Surfaces

Consist of the reachable and exploitable vulnerabilities in a system

Examples:

Open ports on outward facing Web and other servers, and code listening on those ports	Services available on the inside of a firewall	Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats	Interfaces, SQL, and Web forms	An employee with access to sensitive information vulnerable to a social engineering attack

Attack Surface Categories

Network Attack Surface

- Vulnerabilities over an enterprise network, wide-area network, or the Internet
- Included in this category are network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks

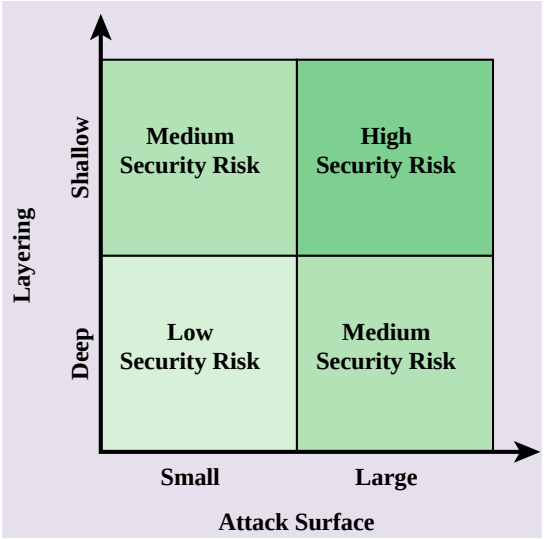
Software Attack Surface

- Vulnerabilities in application, utility, or operating system code
- Particular focus is Web server software

Human Attack Surface

- Vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders

Defense in Depth and Attack Surface



Computer Security Strategy

Specification & policy

- what is the security scheme supposed to do?

Implementation & mechanisms

- how does it do it?

Correctness & assurance

- does it really work?

Computer Security Strategy

Security Policy

- Formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources

Security Implementation

- Involves four complementary courses of action:
  - Prevention
  - Detection
  - Response
  - Recovery

Assurance

- The degree of confidence one has that the security measures, both technical and operation, work as intended to protect the system and the information it processes

Evaluation

- Process of examining a computer product or system with respect to certain criteria