Introduction to Computer Security

Andy Podgurski
Professor
EECS Dept.
Case Western Reserve University

What is Computer Security?

- Computer security is the protection of valued **assets** of a computer system
  - e.g., hardware, software, data, people, processes
- The value of an asset depends on the owner's or user's *perspective*
- It is also *time-dependent*

Basic Security Terminology

- **Threat**: set of circumstances with potential to cause loss or harm
- **Vulnerability**: weakness in a system that could be exploited to cause loss or harm
- **Attack**: deliberate attempt to exploit a vulnerability
- **Control** or **countermeasure**: action, mechanism, procedure, service, or technique that removes or reduces a vulnerability
- A threat is **blocked** by control of a vulnerability

C-I-A Triad or Security Triad

- **Confidentiality**: ability of a system to ensure that an asset is viewed only by authorized parties
- **Integrity**: ability of a system to ensure that an asset is modified only by authorized parties
- **Availability**: ability of a system to ensure that an asset can be used by any authorized parties when needed

Other Desirable Security Properties

- **Authentication**: ability of a system to confirm the identity of a sender
- **Nonrepudiation** or **accountability**: ability of a system to confirm that a sender cannot (convincingly) deny having sent something
- **Auditability**: ability of a system to trace all actions related to a given asset

Confidentiality

- Only *authorized* people or systems can access protected data
  - **Subject:** person, process, or program authorized to access data in particular way
  - **Object:** data item
  - **Access mode:** kind of access
  - **Policy:** authorization
- *Question:* Who authorizes?

Integrity

- Means different things in different contexts:
  - Precise
  - Accurate
  - Unmodified
  - Modified only in acceptable ways
  - Modified only by authorized people or processes
  - Consistent
  - Meaningful and usable

Availability

- Applies to both *data and services*
- May mean different things to different people, e.g.:
  - Object or service is present in *usable* form
  - Service has *adequate capacity*
  - Resources are *fairly allocated*
  - Responses to requests are *timely*
- Achieving availability may require *concurrency control* and *fault tolerance*

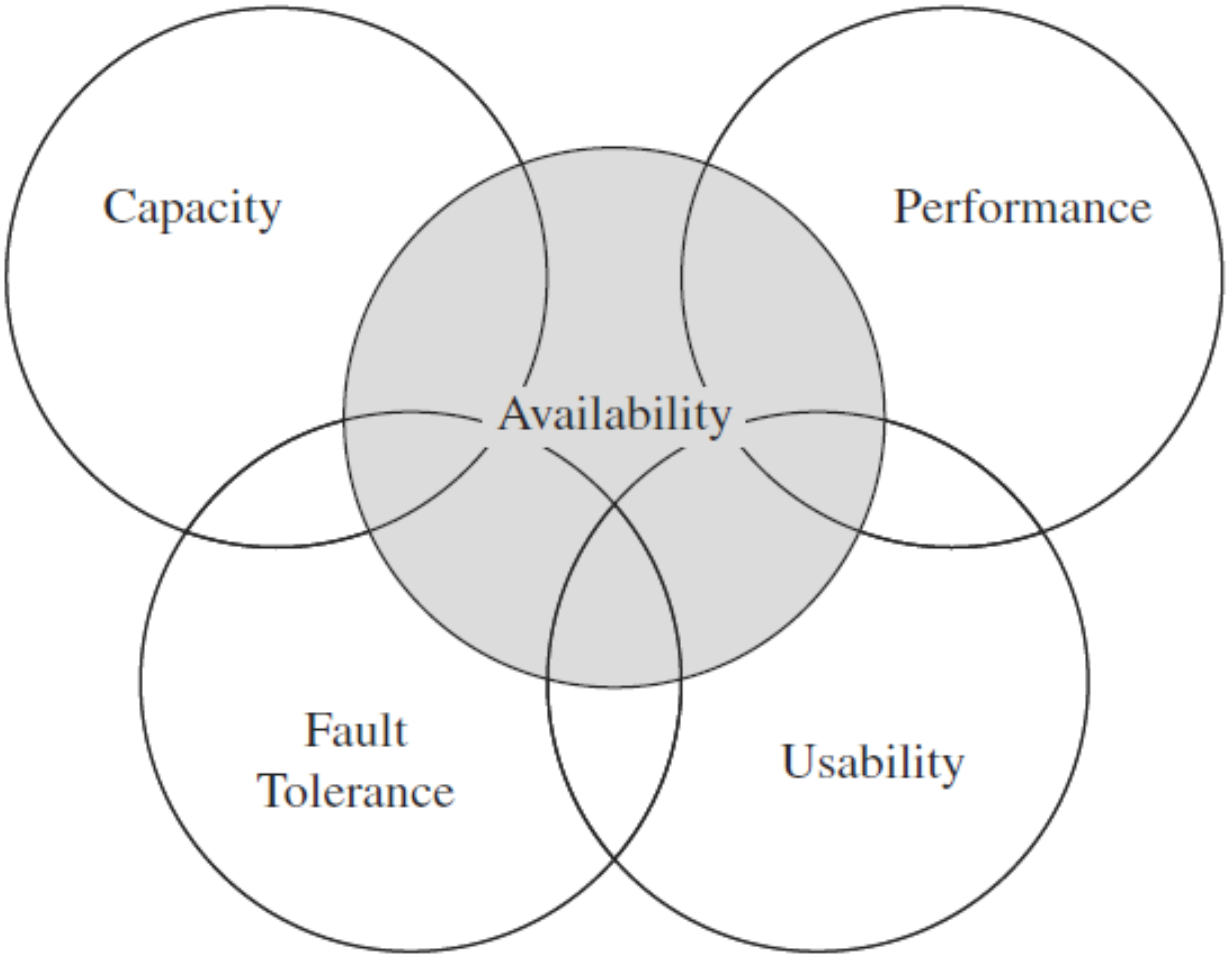

FIGURE 1-7 Availability and Related Aspects

Security Policies and Controls

- **Security policy**: specification of allowed and disallowed activities
  - *Enforced by security controls*
- Example policy: no user should access another's files without permission
- Example security controls:
  - Password authentication
  - OS file access permissions
  - Anti-virus software
  - Encryption
  - Firewalls
  - Intrusion detection systems

Secure System

- Security policy must address all threats
- Security controls must implement entire policy
- Controls must be implemented and administered correctly

Types of Threats

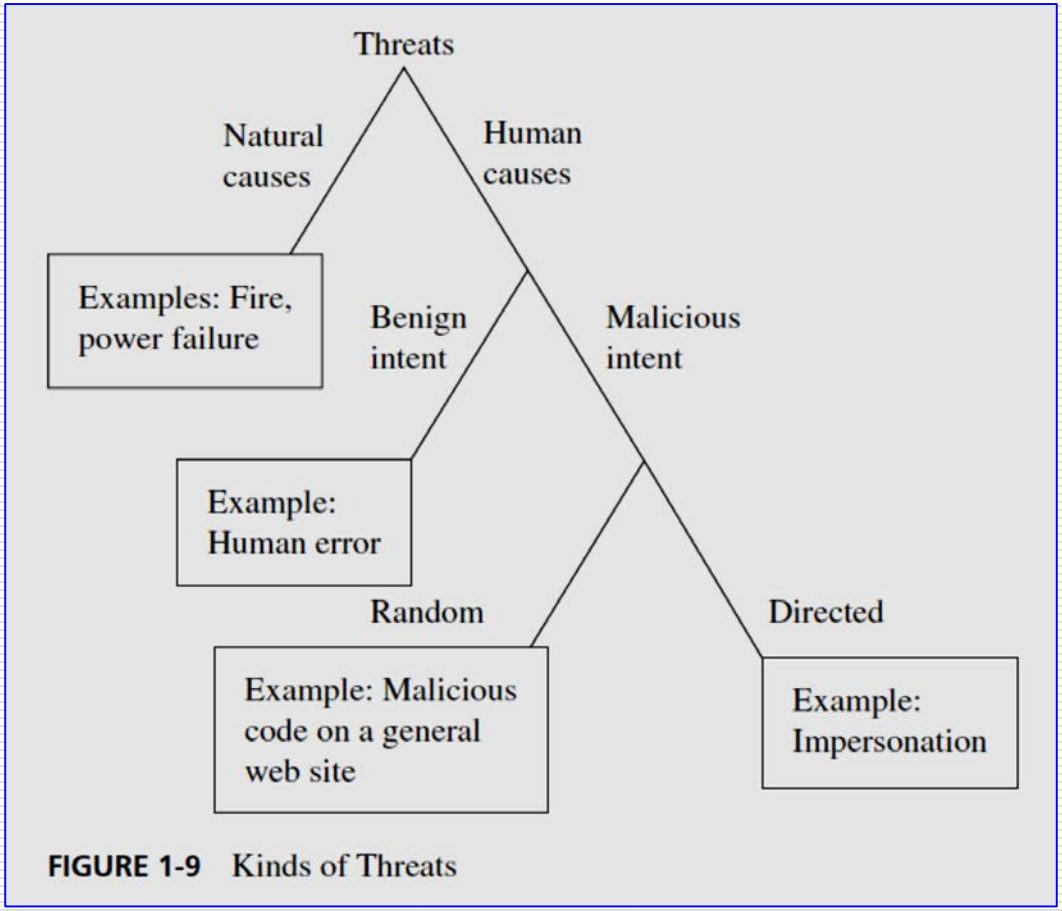

FIGURE 1-9 Kinds of Threats

Common Vulnerabilities

- **Memory safety violations**, e.g.:
  - Buffer overflows
  - Dangling pointers
- **Input validation errors**, e.g.:
  - Format string attacks
  - Improperly handling shell meta-characters so they are interpreted
  - SQL injection
  - Code injection
  - E-mail injection
  - Directory traversal
  - Cross-site scripting in web applications
  - HTTP header injection
  - HTTP response splitting

en.wikipedia.org/wiki/Vulnerability_(computing)

Common Vulnerabilities cont.

- **Race conditions**, e.g.:
  - Time-of-check-to-time-of-use bugs
  - Symlink races
- **Privilege-confusion** bugs, e.g.:
  - Cross-site request forgery in web applications
  - Clickjacking
  - FTP bounce attack
- **Privilege escalation**
- **User interface failures**, e.g.:
  - Warning fatigue or user conditioning
  - Blaming the Victim—prompting a user to make a security decision without giving the user enough information to answer it

en.wikipedia.org/wiki/Vulnerability_(computing)

Types of Attackers

- Individuals
- Organized groups
  - Governments
  - Organized crime
  - “Hacktivists” (e.g., *Anonymous*)
  - Terrorists

avwos.thespudd.com/wp-content/uploads/2015/03/Computer-Cat.jpg

Security Attacks: General Categories

- **Interruption**: asset of system is destroyed or becomes unavailable
- **Interception**: unauthorized party gains access to asset
- **Modification**: unauthorized party tampers with asset
- **Fabrication**: unauthorized party inserts counterfeit objects into system

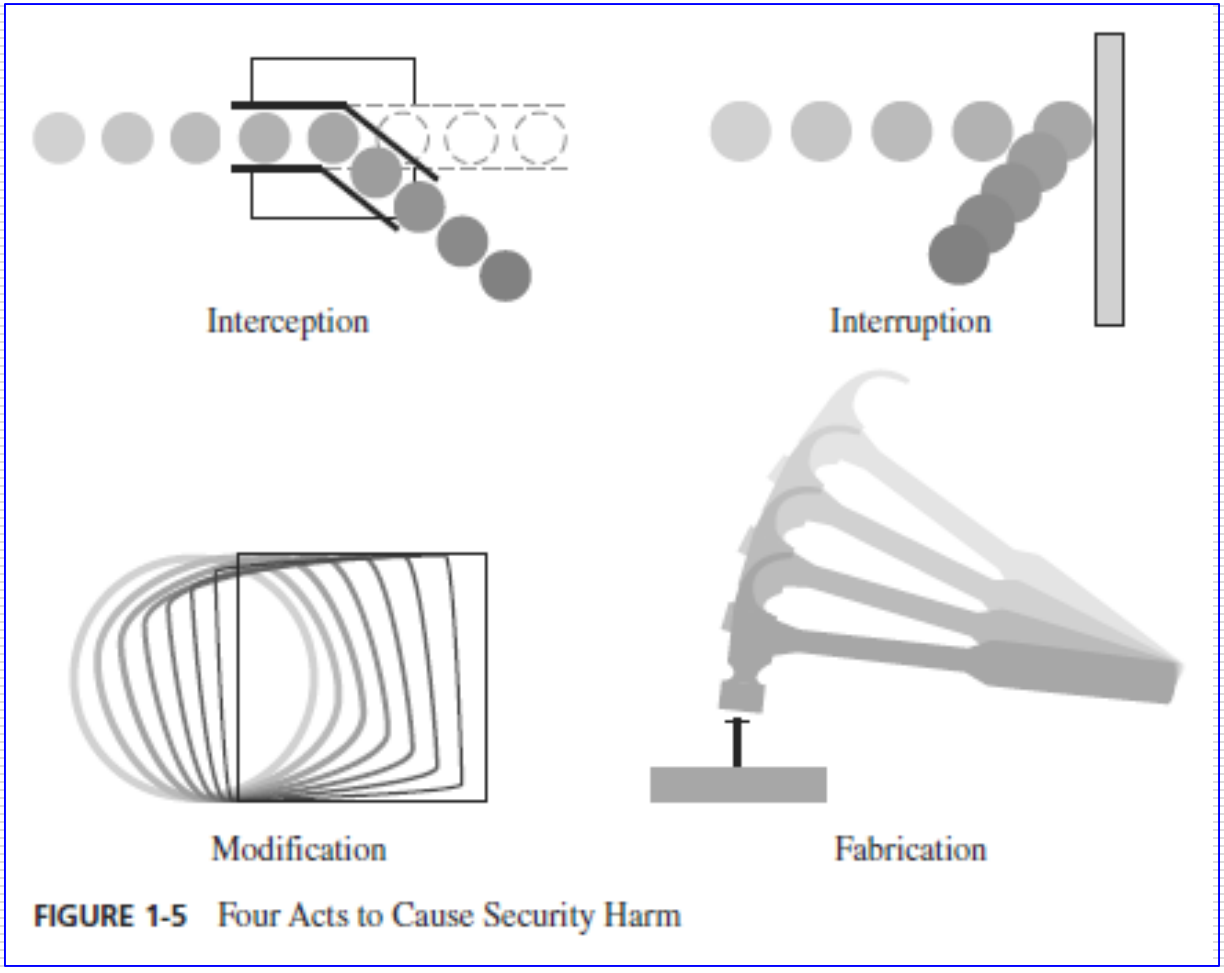

FIGURE 1-5 Four Acts to Cause Security Harm

Pfleeger et al., *Security in Computing*, 5th edition

Active Attacks

- Denial of service (DOS)
- Breaking into a site
  - Information gathering
  - Resource usage
  - Deception
- Replay and modification of messages
- Masquerade

Passive Attacks

- Sniffing
  - Passwords
  - Network traffic
  - Sensitive information
- Information gathering
- Network traffic analysis

Attacker's Process [Cole]

- Passive reconnaissance
- Active reconnaissance (scanning)
- Exploiting the system
  - Gaining access
    - OS attacks
    - Application-level attacks
    - Script and sample program attacks
    - Misconfiguration attacks
  - Elevation of privileges
  - Denial of service
- Uploading programs
- Downloading data
- Keeping access
  - Back doors
  - Trojan horses
- Covering tracks

Attack Routes [Cole]

- Ports
- Services
- Third-party software
- Passwords
- Back doors
- Trojan horses
- Inference channels/covert channels

Methods of Defense

- Encryption
- Software controls
  - Internal program controls
  - OS controls
  - Development controls
  - Antivirus software
  - Event logs
  - Intrusion detection software
- Hardware controls
- Policies
- Physical controls
- Monitoring

Security Assurance

- Ensuring that entity meets its security requirements
  - *Specification* of desired and unacceptable behaviors
  - *Analysis and testing* of
    - Design and implementation of hardware and software
    - Policies and procedures

    to assess conformance to specification
  - *Arguments or proofs* that implementation, operating procedures, and maintenance procedures will produce desired behavior

Human Factors

- Lack of understanding of security threats
- Lack of clear responsibility for security
- Lack of resources
- Untrained personnel
- Disgruntled personnel
- “Social engineering” by attackers

Sources

- *Computer Security: Art and Science* by M. Bishop
- *Hackers Beware* by E. Cole
- *Security in Computing* by C.P. Pfleeger et al.
- *Hacking: The Art of Exploitation* by J. Erickson
- *Hacking Exposed* by J. Scambray and S. McClure
- *Cryptography and Network Security* by W. Stallings