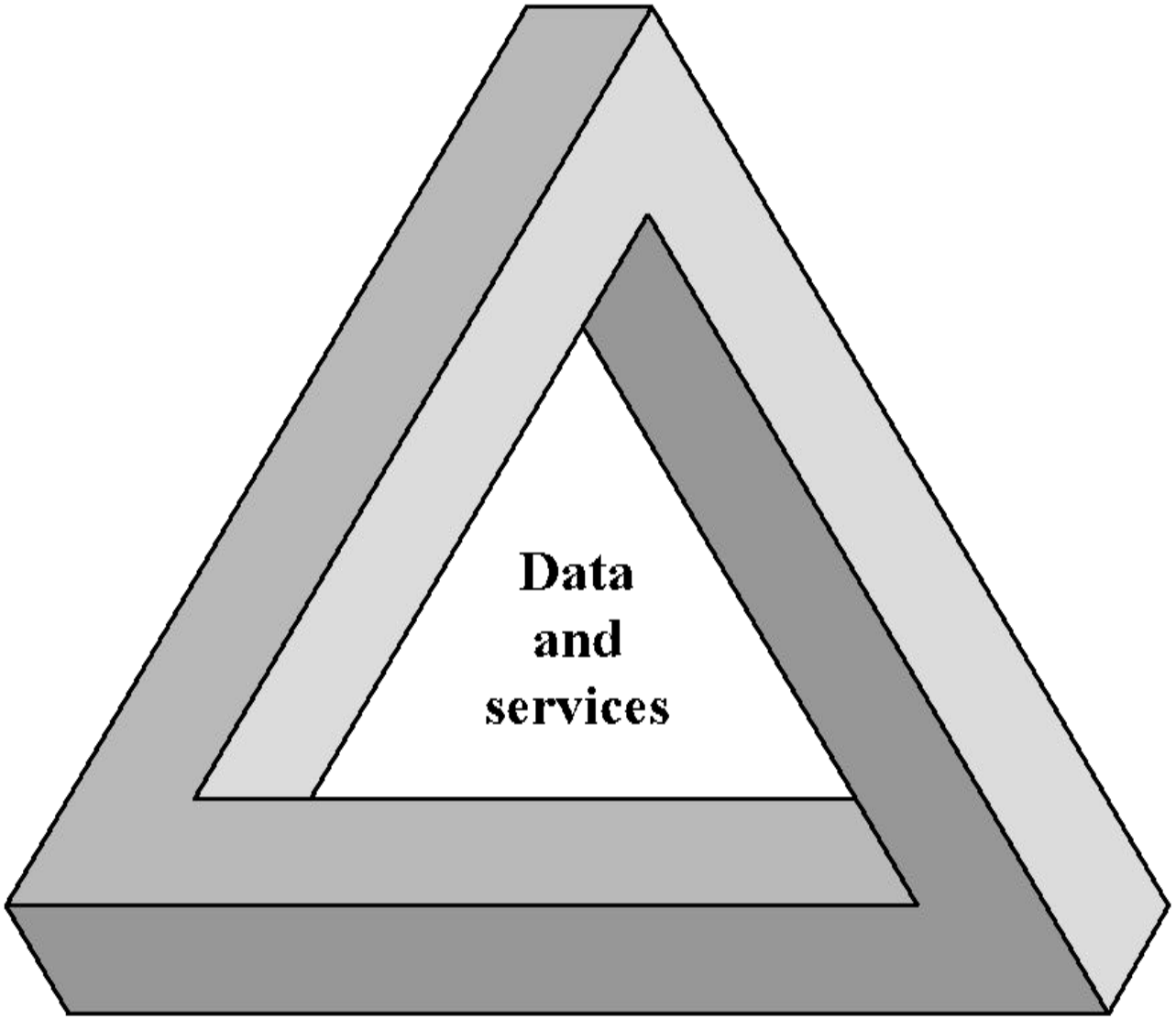
CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

# Computer Security Principles

Lecture 2: Information Security Concepts

# The CIA Triad



# Key Security Concepts

CIT

## Confidentiality

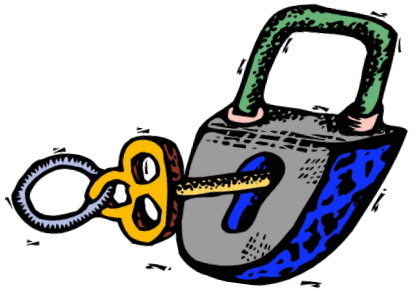
- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

## 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



# Levels of Impact

## Low

The loss could be expected to have a limited 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

## High

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
- Additional algorithms or protocols may be involved
- 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

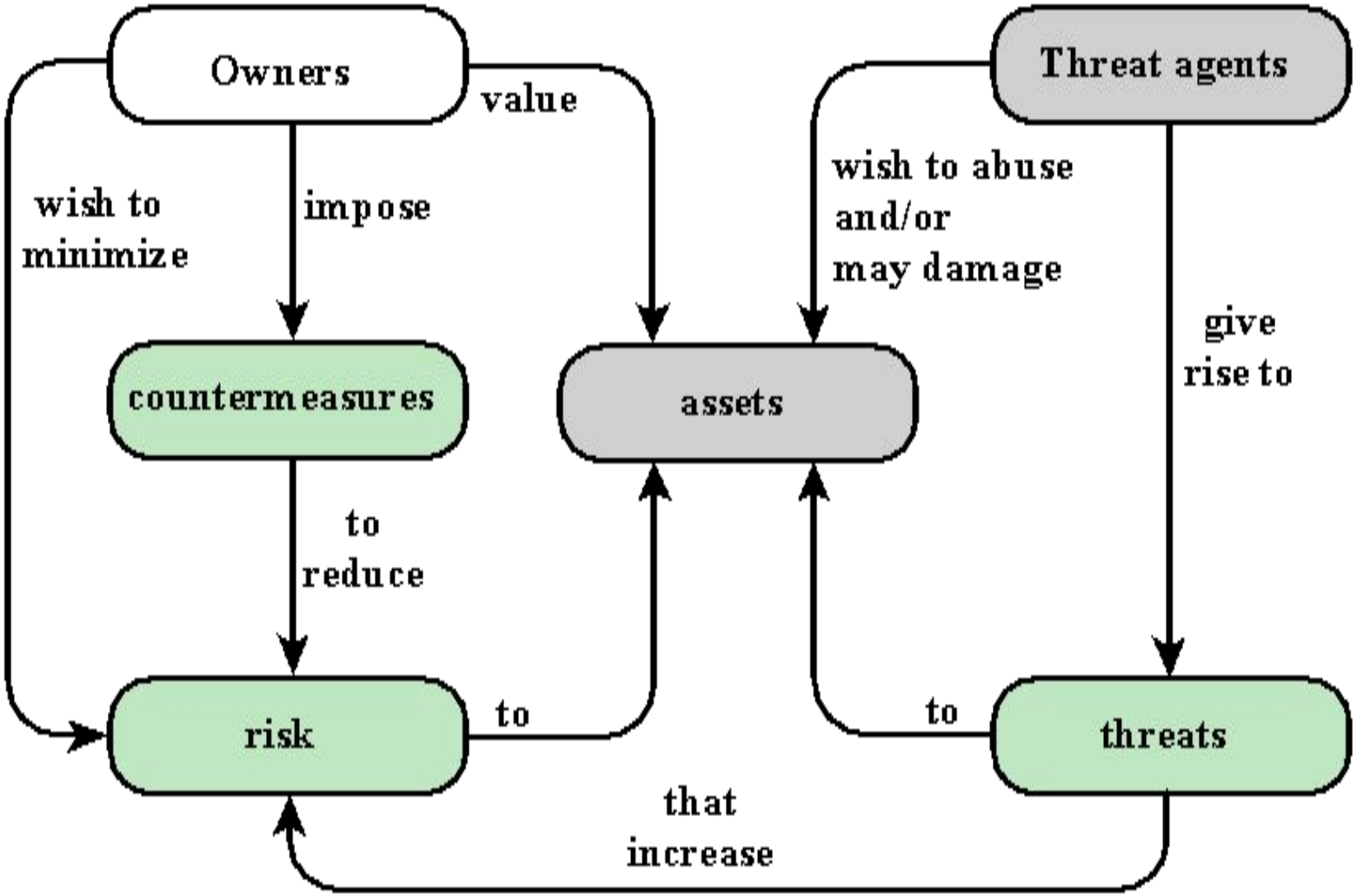
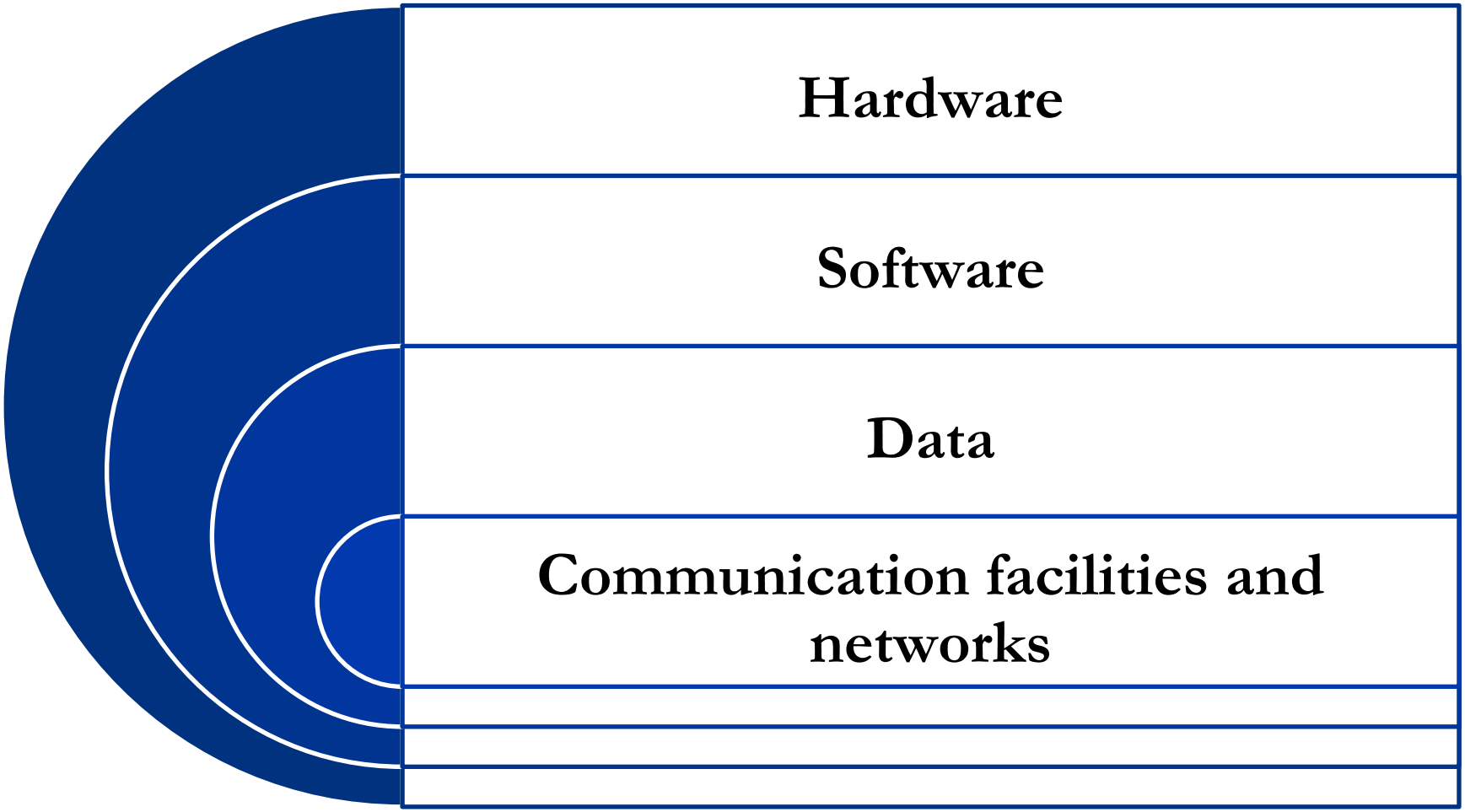



**Figure 1.1 Security Concepts and Relationships**

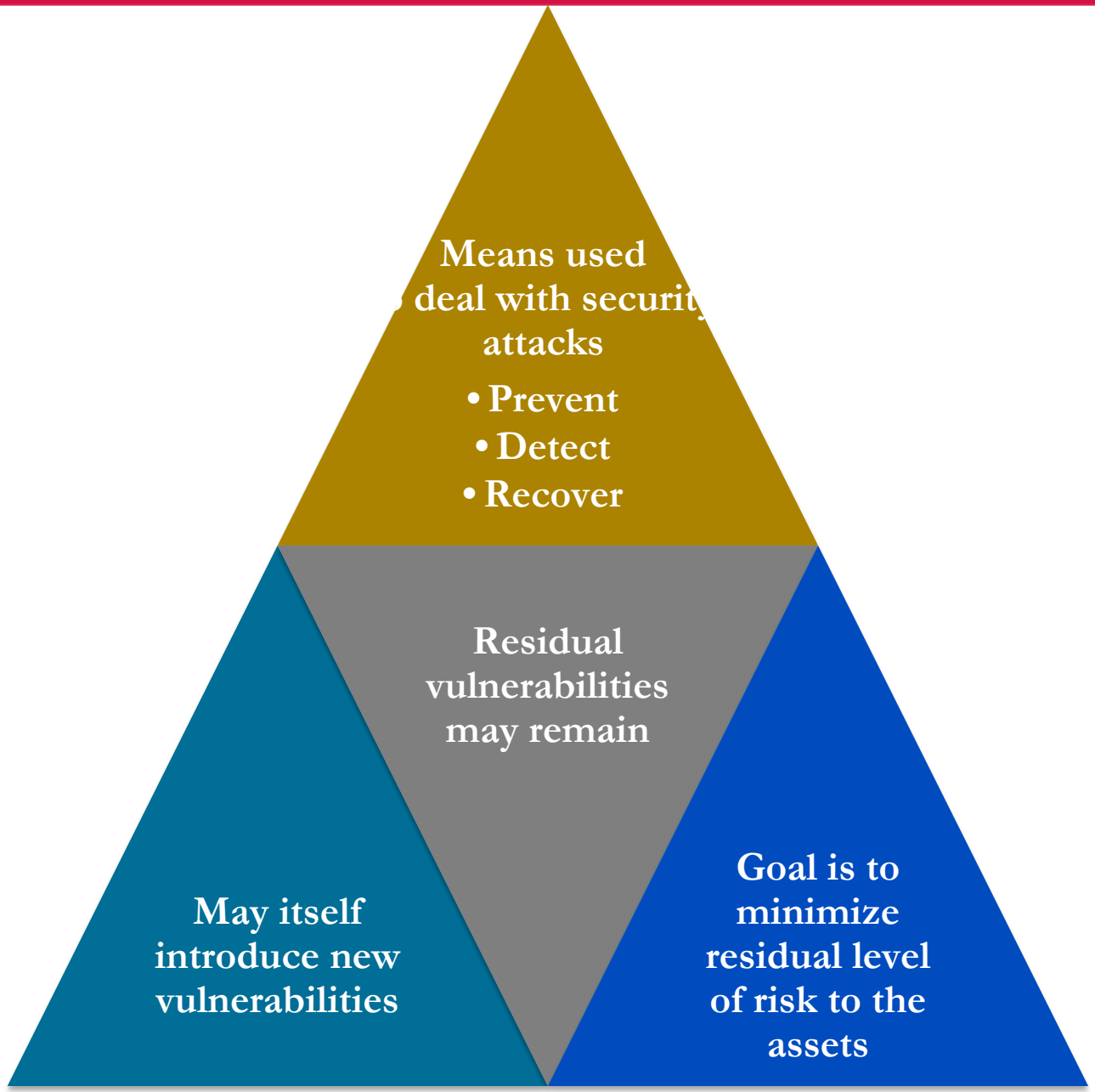
# Asset of a Computer System



# 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

# Countermeasures



| Threat Consequence | Threat Action (Attack) |
|---|---|
| **Unauthorized Disclosure**<br>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.<br>**Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations.<br>**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 byproducts of communications.<br>**Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections. |
| **Deception**<br>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.<br>**Falsification:** False data deceive an authorized entity.<br>**Repudiation:** An entity deceives another by falsely denying responsibility for an act. |
| **Disruption**<br>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.<br>**Corruption:** Undesirably alters system operation by adversely modifying system functions or data.<br>**Obstruction:** A threat action that interrupts delivery of system services by hindering system operation. |
| **Usurpation**<br>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.<br>**Misuse:** Causes a system component to perform a function or service that is detrimental to system security. |

# Computer and Network Assets: 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 Attack

- Attempts to learn or make use of information from the system but does not affect system resources
- Eavesdropping on, or monitoring of, transmissions
- Goal of attacker is to obtain information that is being transmitted
- Two types:
  - Release of message contents
  - Traffic analysis

## Active Attack

- Attempts to alter system resources or affect their operation
- Involve some modification of the data stream or the creation of a false stream
- Four categories:
  - Replay
  - Masquerade
  - Modification of messages
  - Denial of service

# Fundamental Security Design Principles

CIT

| | | | |
|---|---|---|---|
| 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, & 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

Network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, & various forms of intruder attacks

## Software Attack Surface

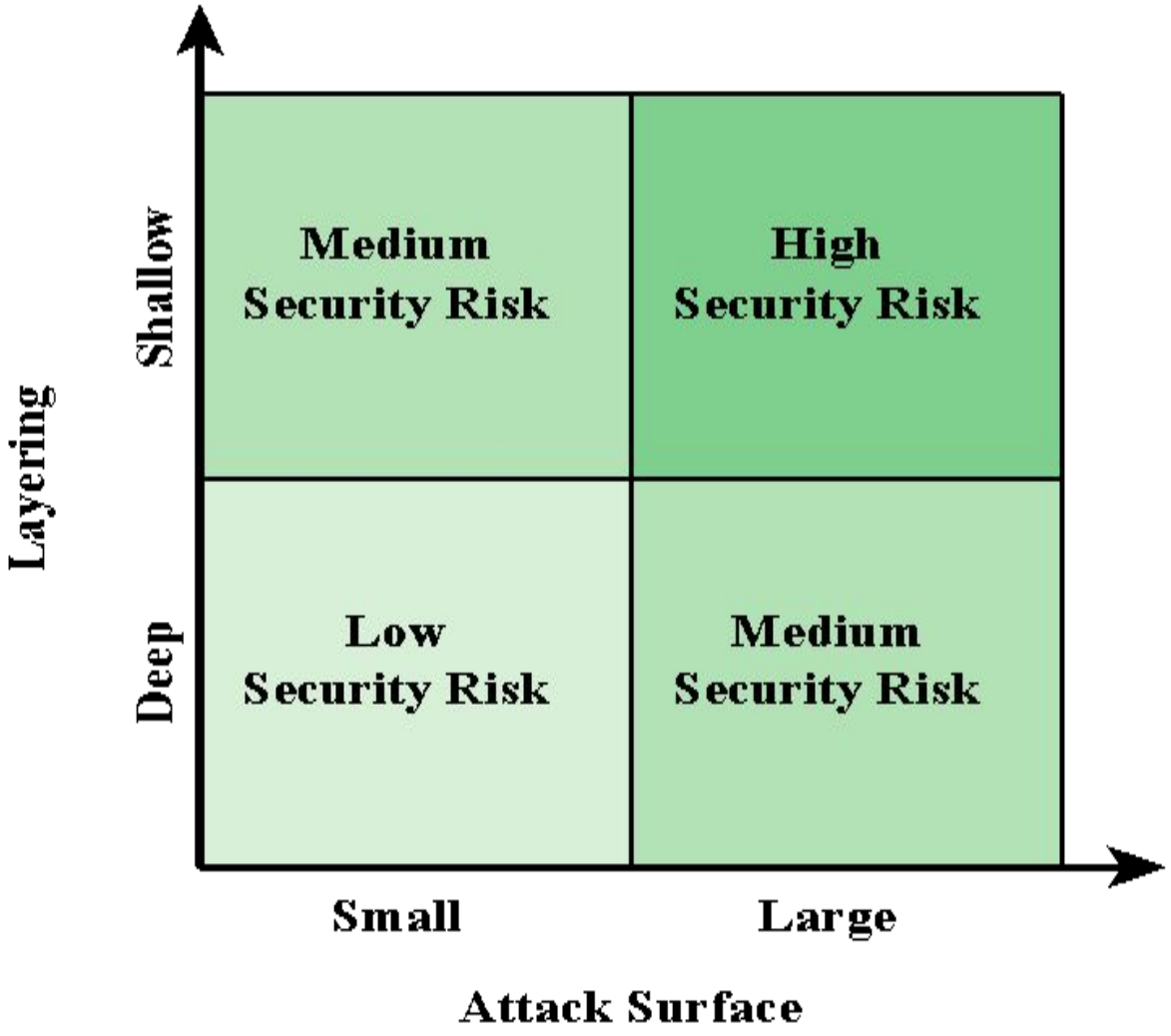
Vulnerabilities in application, utility, or operating system code

Particular focus is Web server software

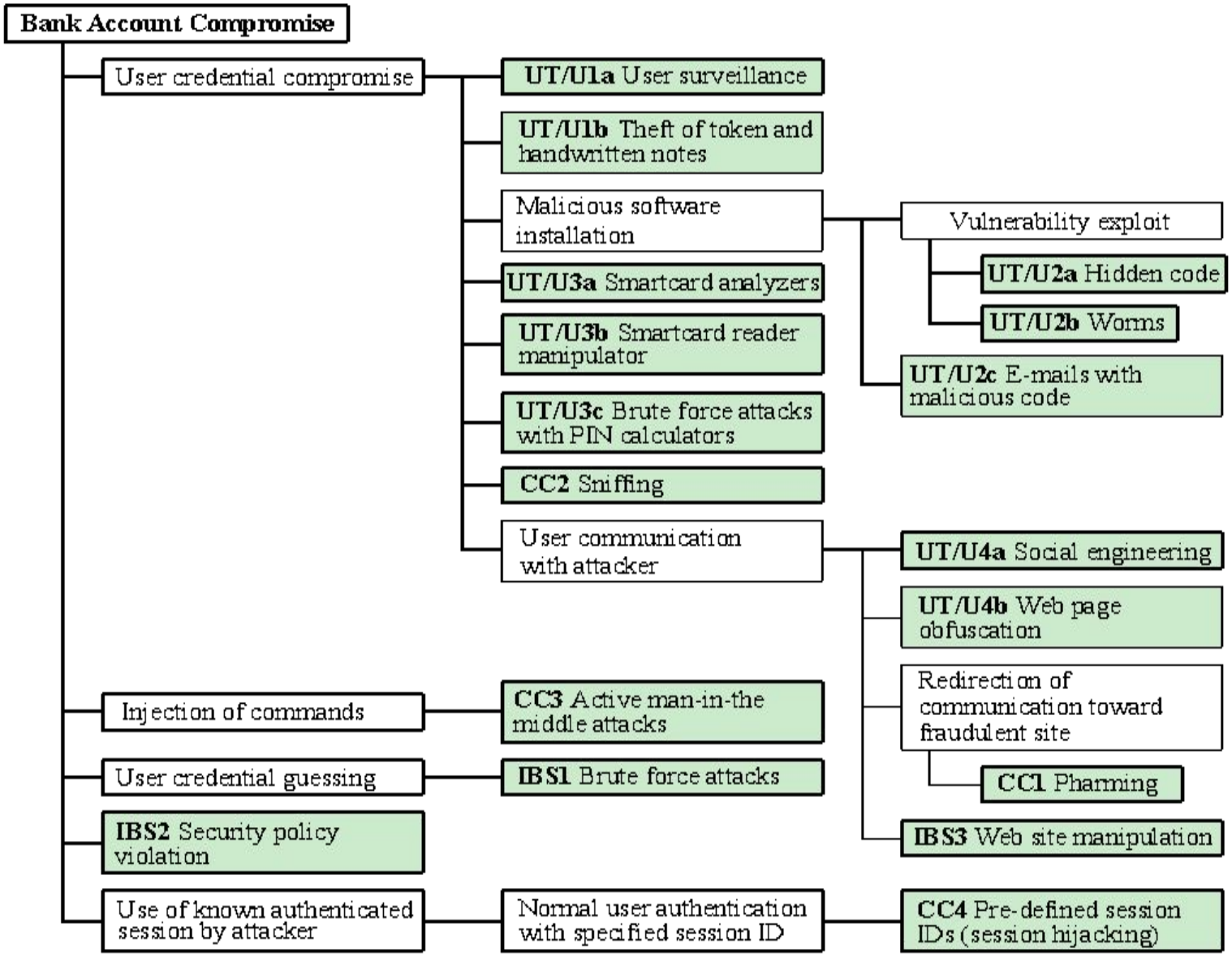
## Human Attack Surface

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

# Defense in Depth and Attack Surfaces



# Internet Banking Authentication Attack Tree



# 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 operational, 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