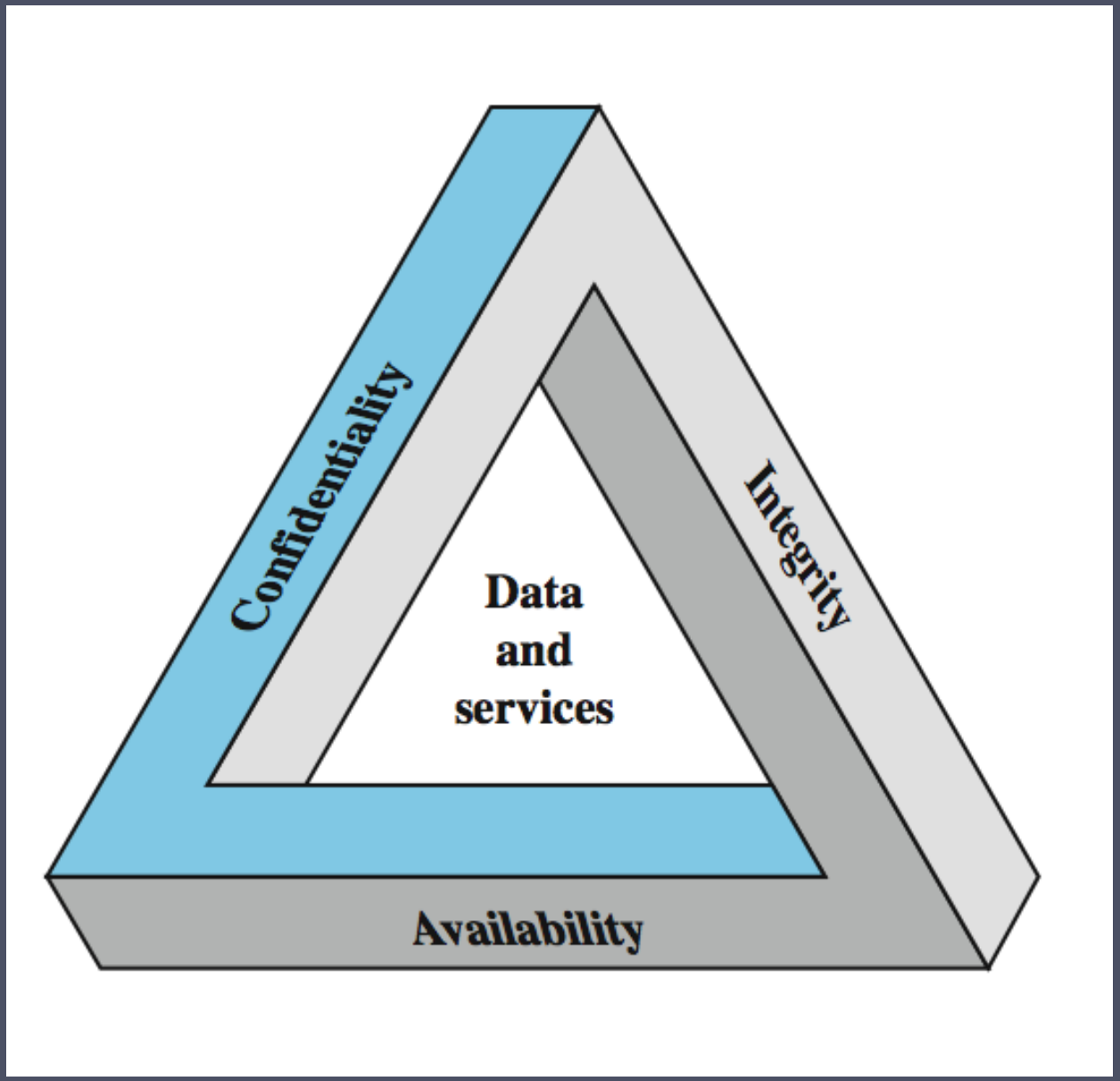
# CNET233SL – Network Security

saliya@nsbm.lk

# What is Network Security:

**Cisco:** "Network security" refers to any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network."

# The CIA Triad



# Key Security Concepts

## Confidentiality

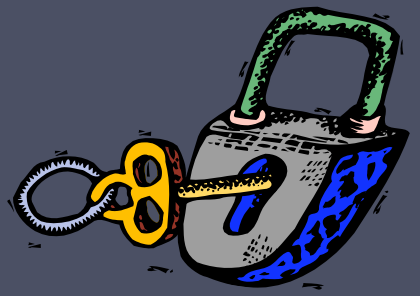
- **Preserving authorized restrictions on information access and disclosure,** including means for protecting personal privacy and proprietary information

## 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**



# Additional Security Concepts

- Authenticity: This means verifying that users and entities are who they say they are and that each input arriving at the system came from a trusted source.
- Accountability: Keeping recodes of activities done by various users & entities in a computing system.
  - Because truly secure systems aren't yet an achievable goal, we must be able to trace a security breach to a responsible party.
  - Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

# 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

# Computer Security Terminology

## Based on RFC 4949, *Internet Security Glossary*, May 2000

- **Adversary (threat agent):** An entity that attacks a system. Or an entity that pose a threat to a system
- **Attack:** An assault on system security. This should be an intelligent and deliberate attempt to violate security of a system
- **Countermeasure:** An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack
- **Risk: T**he probability of loss of security related to particular threat and a particular vulnerability
- **Security Policy:** A set of rules and practices imposed to protect sensitive and critical system resources
- **System Resource (Asset):** Data contained in an information system; or a service provided by a system; or a system capability
  - E.g. processing power or communication bandwidth
- **Threat:** A potential for violation of security. That is, a threat is a possible danger that might exploit a vulnerability
- **Vulnerability:** A security flaw or weakness in a system's design, implementation, or operation and management

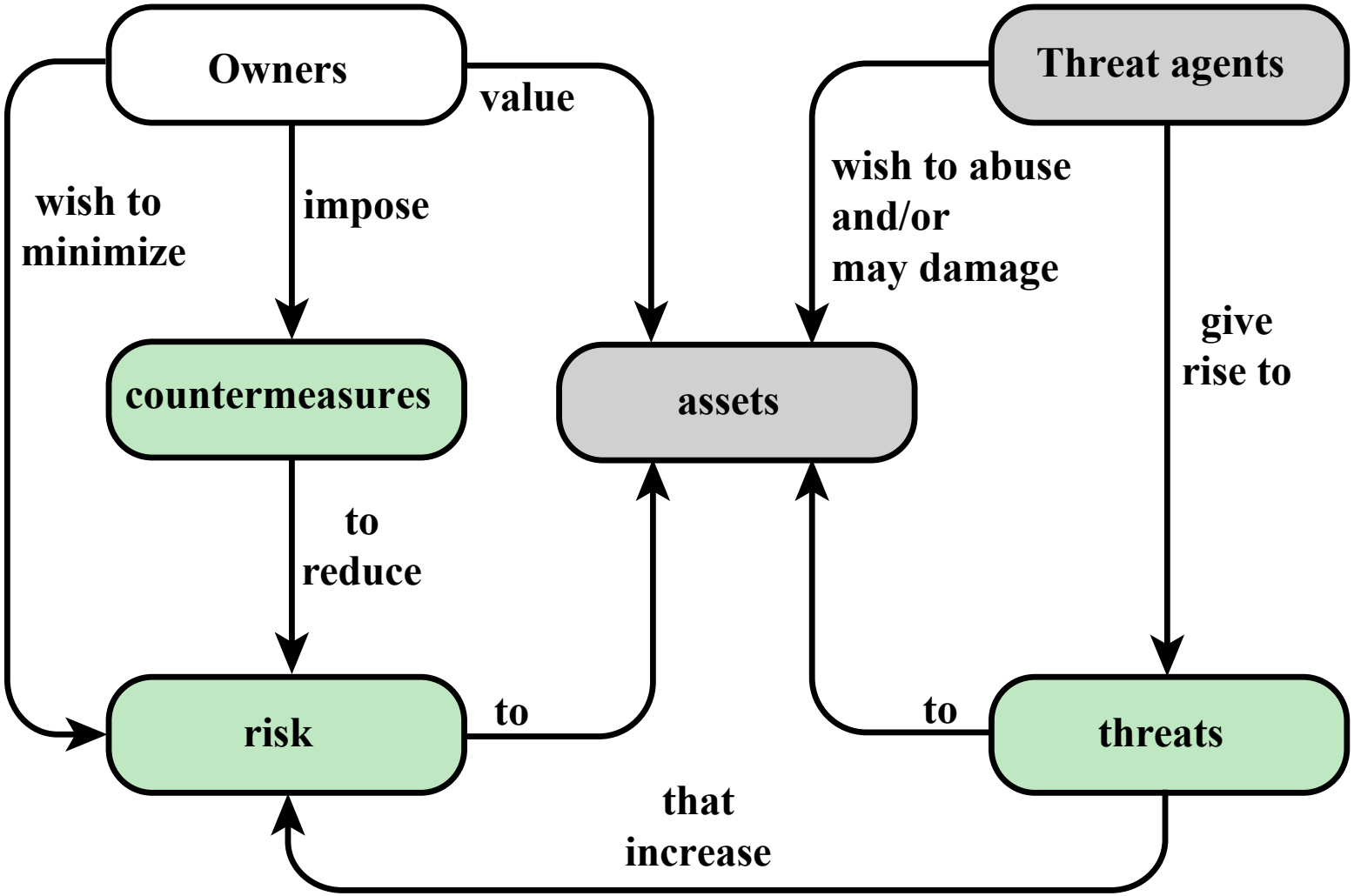
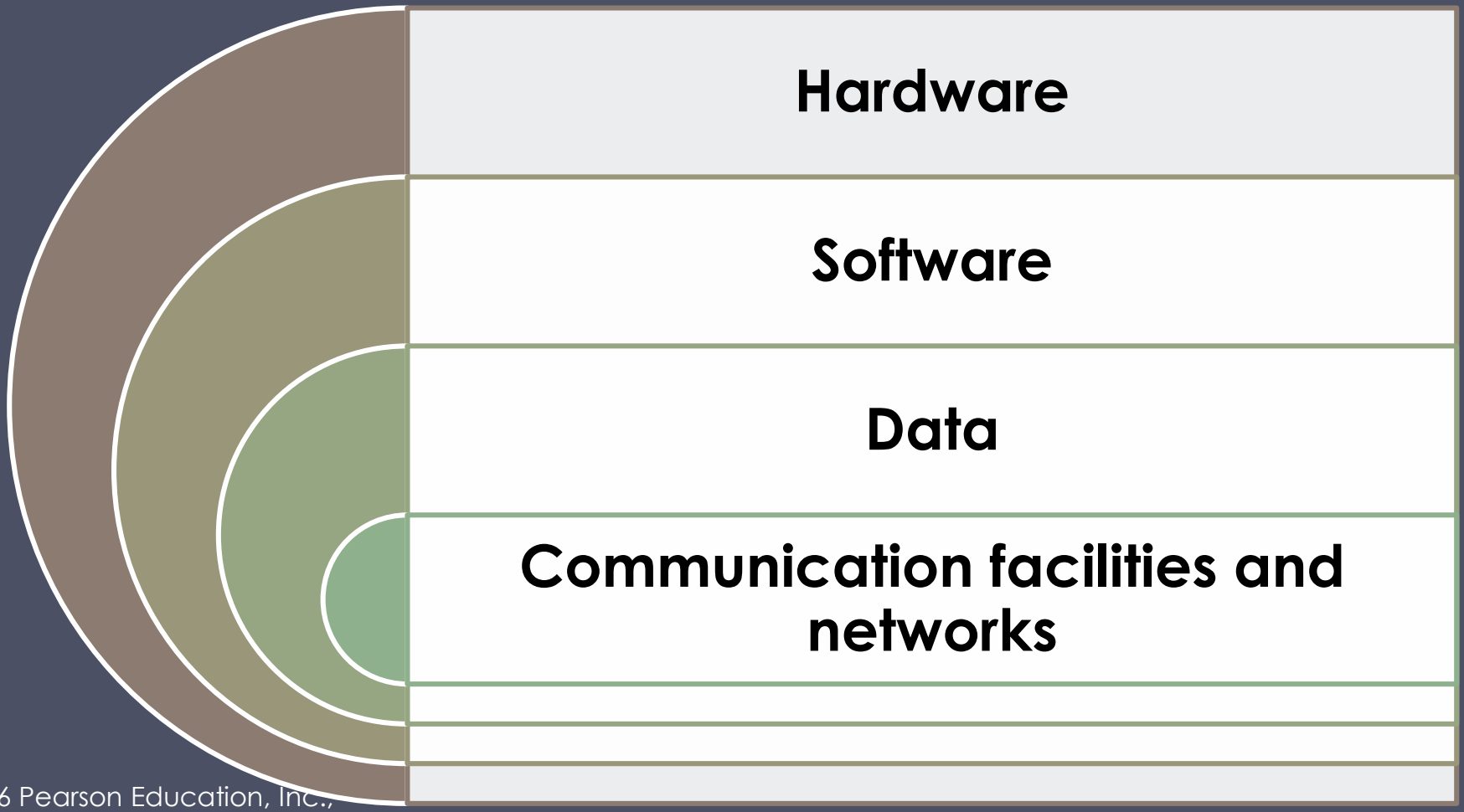


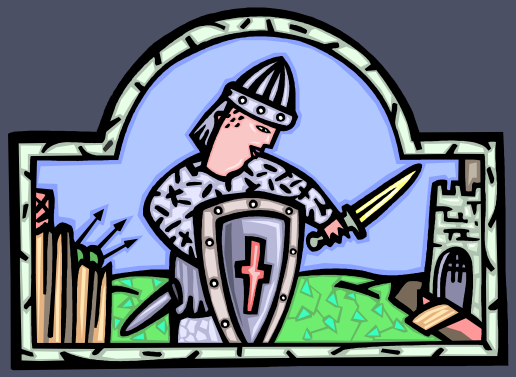

**Figure 1.1 Security Concepts and Relationships**

# Assets of a Computer System



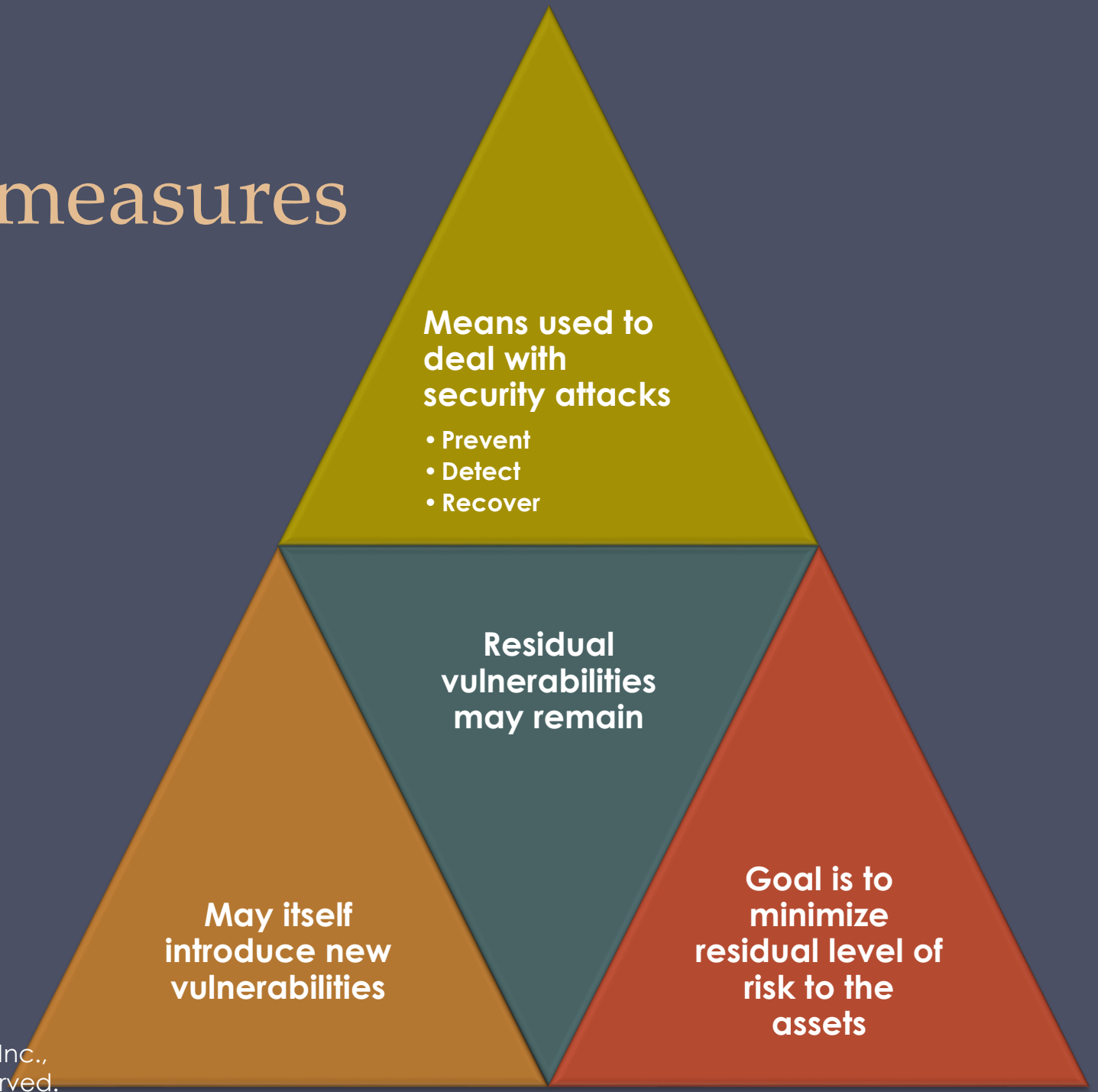
# Vulnerabilities, Threats and Attacks

- Few Categories of vulnerabilities
  - software
    - insufficient testing
    - lack of audit trail
  - network
    - unprotected communication lines
    - insecure network architecture



- 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 perimeter
  - 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 unauthorized data | **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. |

# Table 1.2

Threat Consequences, and the Types of Threat Actions That Cause Each Consequence

Based on RFC 4949

**Table is on page 20 in the textbook.

# Table 1.3
## Computer and Network Assets, with Examples of 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

# Security Requirements
## (Based on FIPS PUB 200)

- **Access Control:** Limit information system access to authorized users
- **Awareness and Training**:
  - (i) Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities. Also they made aware of the applicable laws, regulation, and policies related to the security of organizational information systems; and
  - (ii) ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
- **Audit and Accountability:**
  - (i) Create, protect, and retain information system audit records to enable the monitoring, analysis, investigation, and reporting of inappropriate information system activity; and
  - (ii) ensure that the actions of individual users can be tracked.
- **Contingency Planning:** Establish, maintain, and implement plans for emergency response, backup, and postdisaster recovery to ensure the availability of critical information resources.
- **Identification and Authentication:** Identify users, or devices, and authenticate (or verify) the those identities.
- **Risk Assessment**: Periodically assess the information security risk to organizational operations, organizational assets, and individuals.
- **Etc…**

(Table can be found on page 26 in the textbook.)

# 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 | | | |

# Fundamental Security Design Principles

- **Economy of mechanism:** the design of security measures embodied in both hardware and software should be as simple and small as possible.
- **Fail-safe defaults:** access decisions should be based on permission rather than exclusion.
- **Complete mediation:** every access must be checked against the access control mechanism.
- **Open design:** the design of a security mechanism should be open rather than secret.
- **Separation of privilege:** a practice in which multiple privilege attributes are required to achieve access to a restricted resource. E.g. Smart Card & PIN/Password
- **Least privilege:** every process and every user of the system should operate using the least set of privileges necessary to perform the task.
- **Least common mechanism:** the design should minimize the functions shared by different users, providing mutual security.
- **Psychological acceptability:** Where possible, security mechanisms should be transparent to the users of the system or at most introduce minimal obstruction.

(Table can be found on page 26 in the textbook.)

# Fundamental Security Design Principles

- **Isolation:** a principle that applies in three contexts.
  - First, public access systems should be isolated from critical resources (data, processes, etc.) to prevent disclosure
  - Second, the processes and files of individual users should be isolated from one another except where it is explicitly desired. or tampering.
  - And finally, security mechanisms should be isolated in the sense of preventing access to those mechanisms.
- **Encapsulation:** Relates to object oriented concept. protected subsystem and the procedures may be called only at designated domain entry points.
- **Modularity:** development of security functions as separate, protected modules and to the use of a modular architecture for mechanism design and implementation.
- **Layering:** use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems. This technique is often referred to as defense in depth.
- **Least astonishment:** program or user interface should always respond in the way that is least likely to astonish the user.

(Table 2.1 can be found on page 26 in the textbook.)

# Attack Surfaces

Consist of the reachable and exploitable vulnerabilities in a system

Examples:

- Open ports and code listening on those ports
- Services available on the inside of a firewall
- Code that processes incoming data, email, XML, office documents, etc
- 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, disruption of communications links etc.

## Software Attack Surface

Vulnerabilities in application, utility, or operating system code

Particular focus is Web server software

## Human Attack Surface

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

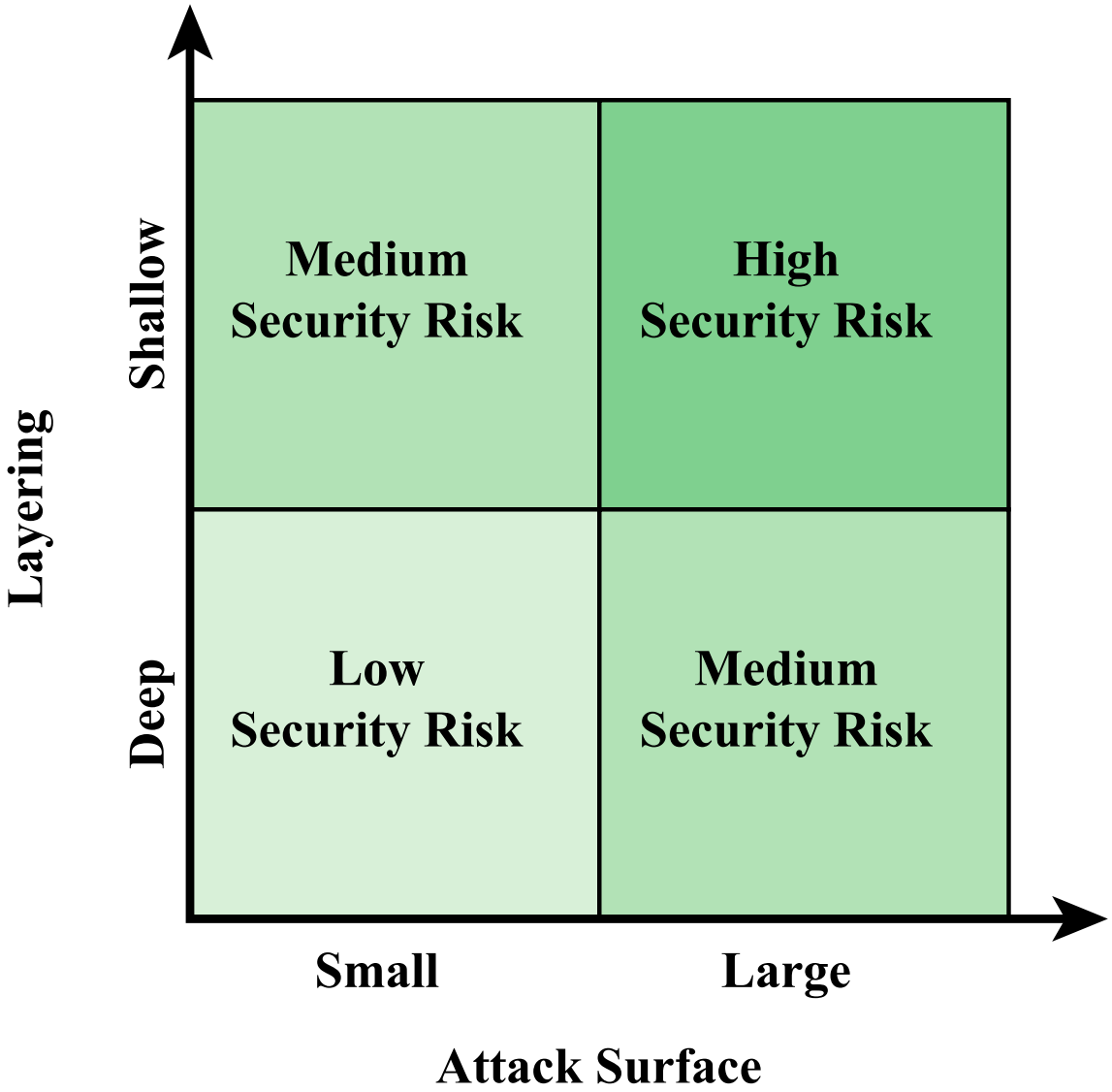



**Figure 1.3 Defense in Depth and Attack Surface**

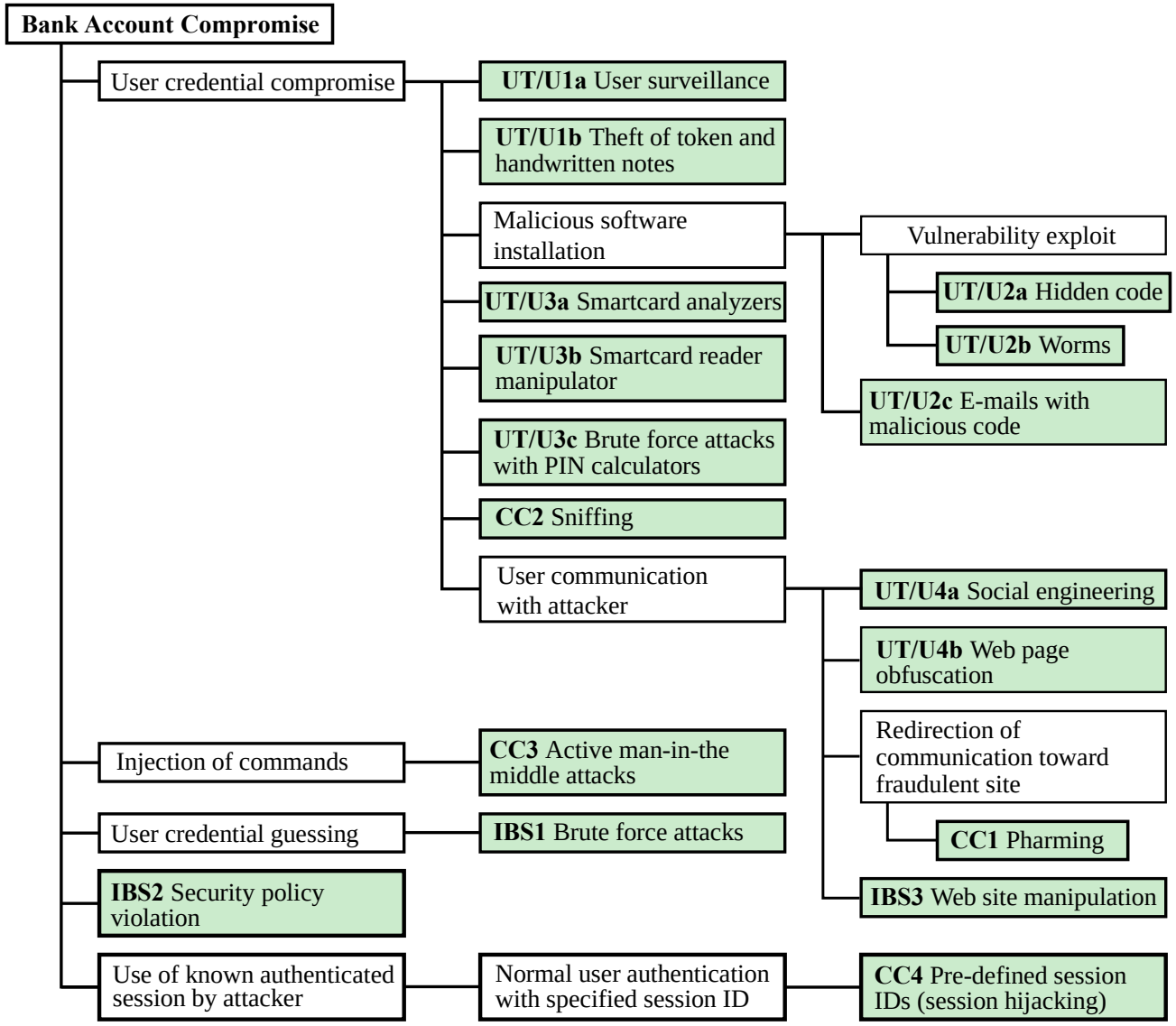
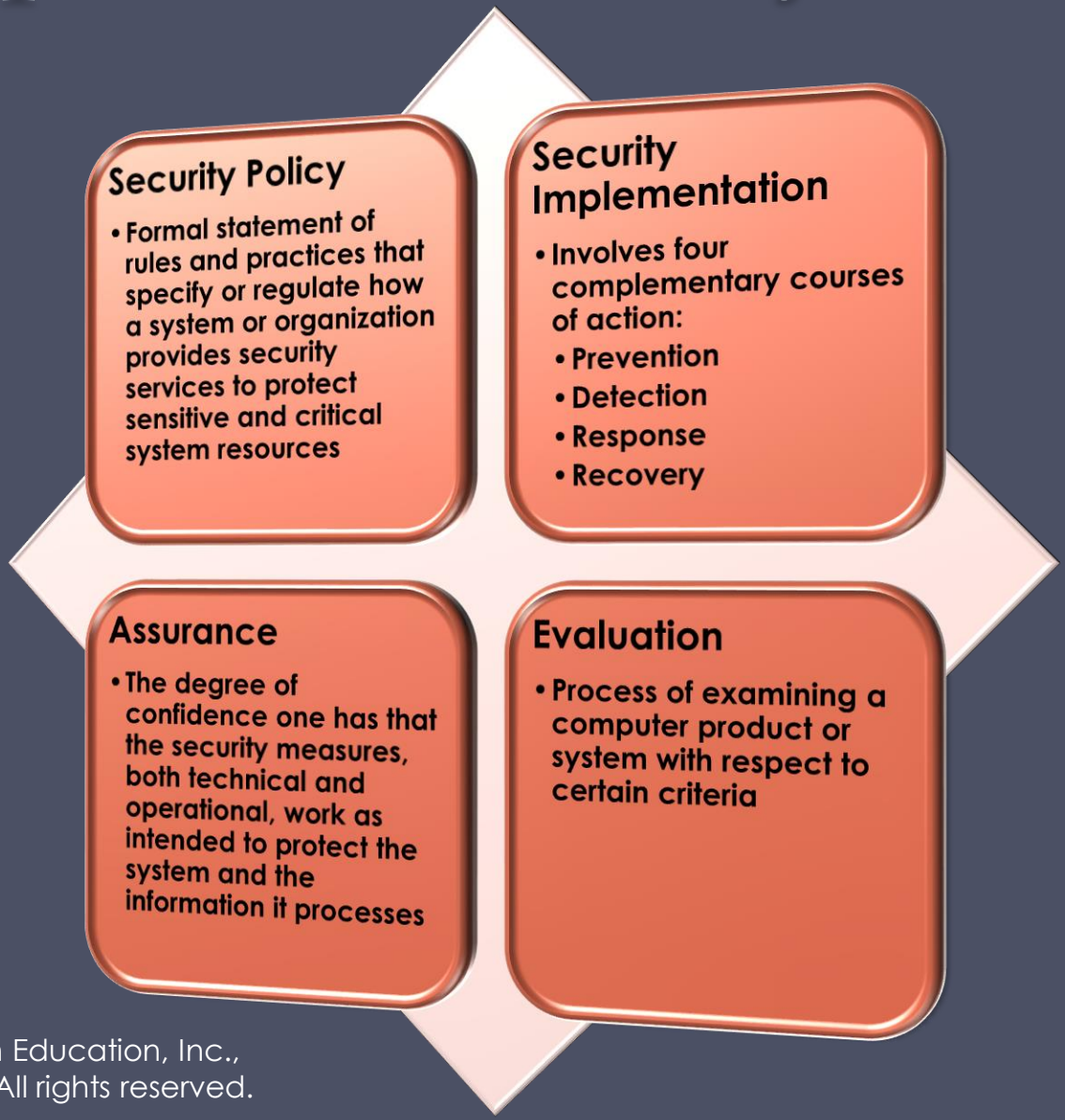



**Figure 1.4 An Attack Tree for Internet Banking Authentication**

- Exercise:
  - Develop an attack tree for gaining access to the contents of a physical safe.

# Computer Security Strategy



# Summary

- Computer security concepts
  - Definition
  - Challenges
  - Model
- Threats, attacks, and assets
  - Threats and attacks
  - Threats and assets
- Security functional requirements

- Fundamental security design principles
- Attack surfaces and attack trees
  - Attack surfaces
  - Attack trees
- Computer security strategy
  - Security policy
  - Security implementation
  - Assurance and evaluation