Overview

- Computer security deals with computer-related assets that are subject to a variety of threats and for which various countermeasures are taken to protect those assets

- The focus of this course is on three fundamental issues
  1. What *assets* do we need to protect?
  2. How are those assets *threatened*?
  3. What can we do to *counter* those threats?

Index

- Computer Security Concepts
- Threats, Attacks, and Assets
- Security Functional Requirements
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- Computer Security Strategy

Learning objectives

- Describe the key security requirements of confidentiality, integrity and availability
- Discuss the types of security threats and attacks that must be dealt with
- Explain the countermeasures that can be taken to deal with such threats and attacks in terms of
  - **functional requirements**
  - **fundamental security design principles**
  - **attack surfaces** and **attack trees**
- Understand the main aspects of a comprehensive security strategy

Index

- Computer Security Concepts
- Threats, Attacks, and Assets
- Security Functional Requirements
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- Computer Security Strategy

A definition of computer security

Computer security:

Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated

The NIST Internal/Interagency Report NISTIR 7298
[Glossary of Key Information Security Terms, May 2013]
(**NIST** = U.S. National Institute of Standards and Technology)

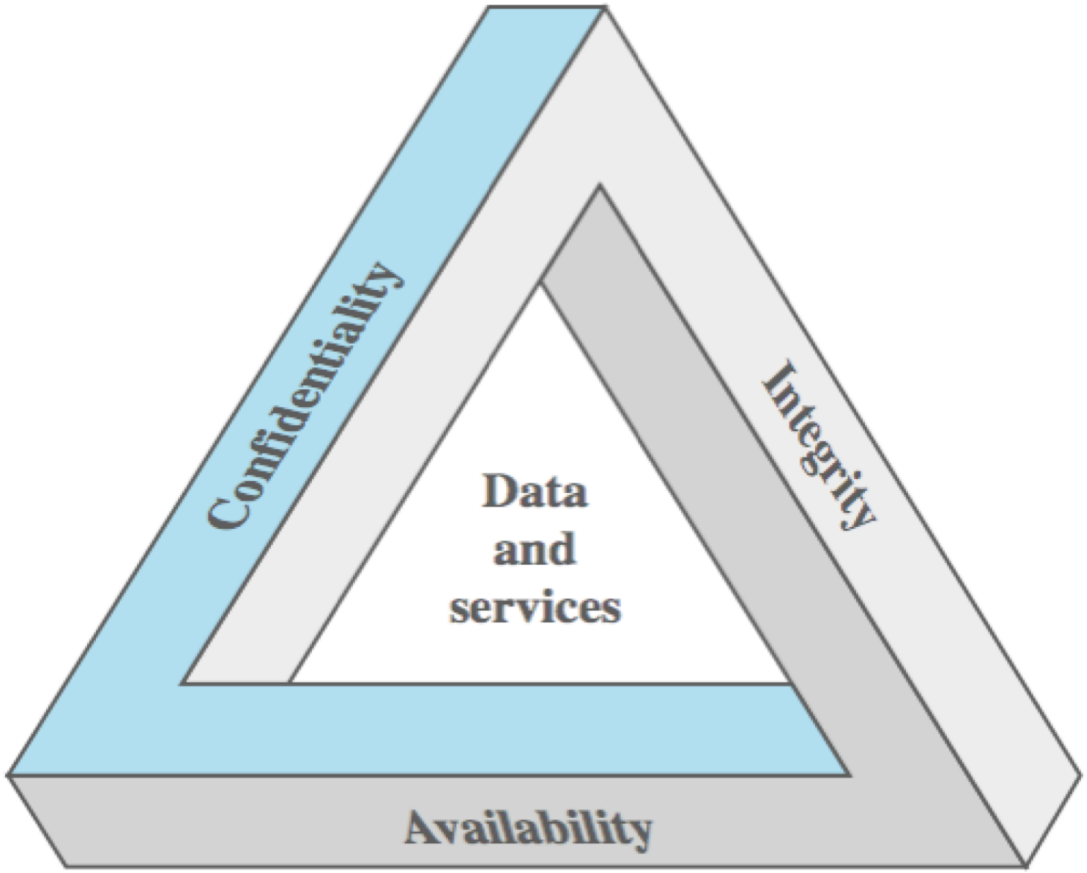
Three key objectives

- Confidentiality: this term covers two related concepts
  - **Data confidentiality**: Assures that confidential information is not disclosed to unauthorized individuals
  - **Privacy**: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed
- Integrity: this term covers two related concepts
  - **Data integrity**: Assures that information and programs are changed only in a specified and authorized manner
  - **System integrity**: Assures that a system performs its operations in unimpaired manner, free from unauthorized manipulation
- Availability: Assures that systems work promptly and service is not denied to authorized users

N.B. Security literature typically does not distinguish between data and information

The CIA triad

- **Confidentiality, Integrity, Availability** form what is often referred to as the CIA triad
- The three concepts embody the fundamental security objectives for both data and for information and computing services



Key Security Concepts (the CIA triad)

The NIST standard FIPS 199 (*Standards for Security Categorization of Federal Information and Information Systems, 2004*) provides

- a useful characterization of these three objectives in terms of *requirements*
- the definition of a *loss* of security in each category

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity
- Ensuring timely and reliable access to and use of information

Key Security Concepts (the CIA triad)

The NIST standard FIPS 199 (*Standards for Security Categorization of Federal Information and Information Systems, 2004*) provides

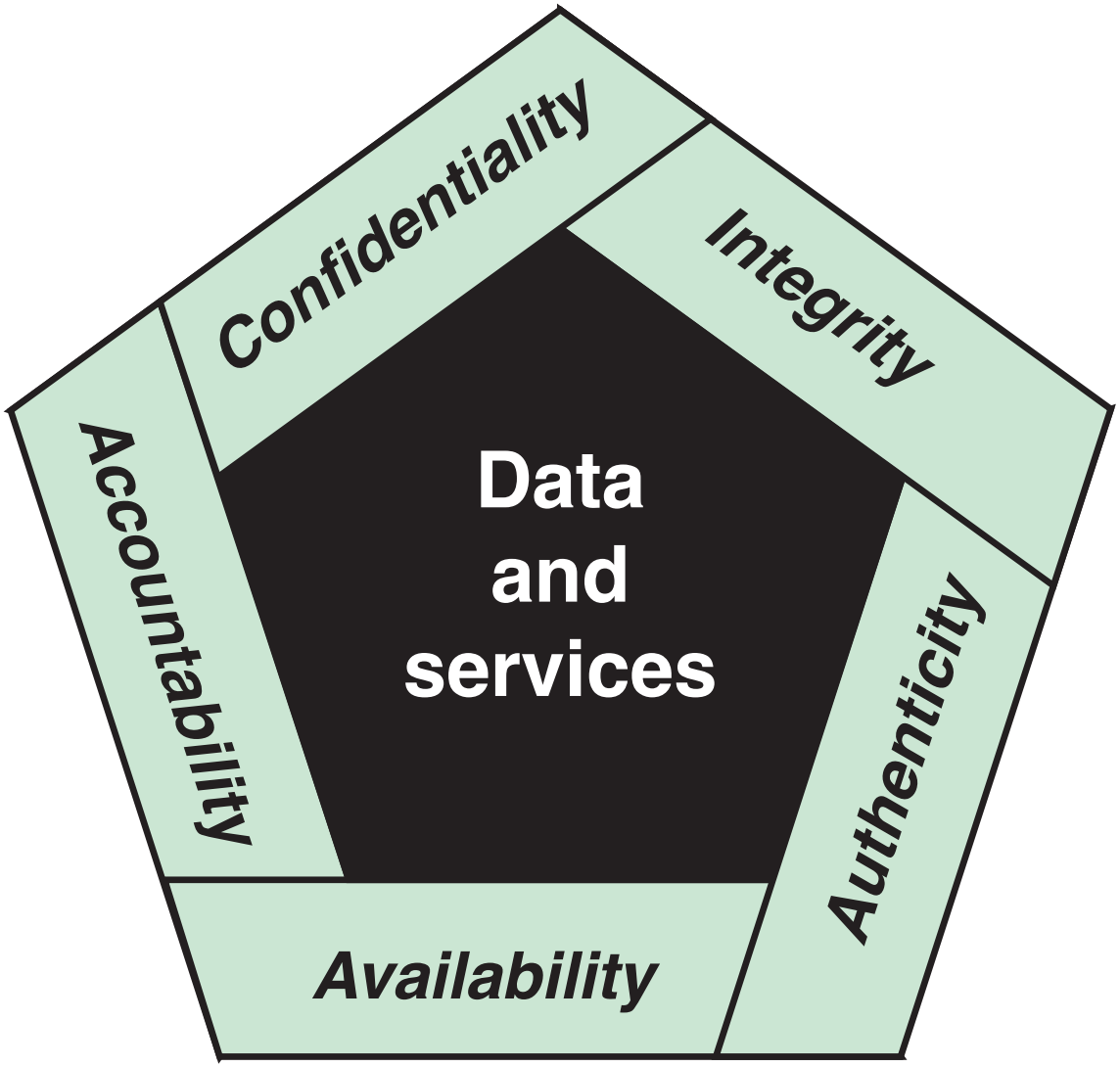
- a useful characterization of these three objectives in terms of *requirements*
- the definition of a *loss* of security in each category

- A *loss* of confidentiality is the unauthorized disclosure of information
- A *loss* of integrity is the unauthorized modification or destruction of information
- A *loss* of availability is the disruption of access to or use of information or an information system

Additional concepts to present a complete security picture

- Authenticity: assures that an entity or object is genuine and able to be verified and trusted
  - Supports confidence in the validity of a transmission, a message, or its originator
- Accountability: assures that actions of an entity can be traced uniquely to that entity
  - Supports nonrepudiation, intrusion detection and prevention, fault isolation, etc.

The CIA triad two plus Additional Concepts



Examples of security requirements

- We now provide some examples of applications that illustrate the requirements just enumerated
- For these examples, we use three levels of impact on organizations or individuals should there be a *breach of security* (that is a loss of confidentiality, integrity, or availability)
  - These levels are defined in FIPS 199

Levels of security breach 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

Examples of security requirements: Confidentiality

- **Student grade information** is an asset whose confidentiality is considered to be very important
  - According to the US Family Education Right and Privacy Act (FERPA): grades should only be available to students, their parents, and employees that require the information to do their job
- **Student enrollment information**
  - Less damage if disclosed
  - Has usually moderate confidentiality rating
- **Directory information**, e.g. lists of students, faculty or departmental lists
  - Often available publicly

Examples of security requirements: Integrity

- **A hospital patient's allergy information**
  - Inaccurate information could result in serious harm or death to a patient and expose the hospital to massive liability
  - A doctor should be able to trust that the info is correct and up-to-date
  - If a nurse deliberately falsifies the data, the database should be restored to a trusted basis and the falsified information traced back to the person who did it
- **An online newsgroup registration data**
  - Moderate level of integrity requirement
- **Anonymous online poll**
  - Inaccuracy is well understood: many Web sites offer these polls to their users with very few safeguards

Examples of security requirements: Availability

- A system that provides **authentication services** for critical systems, applications, and devices
  - The loss of services could result in financial loss for customers
- A **public Web site** for a university that provides information for current and prospective students
  - Not critical, but causes embarrassment
- An **online telephone directory lookup application**
  - Unavailability is mostly annoyance (there are alternative sources, such as a hardcopy directory or the operator)

Computer Security Challenges

Ten *reasons* for which computer security is challenging

1. Computer security is not as simple as it might first appear: The requirements seem to be straightforward, but the mechanisms used to meet those requirements can be quite complex and involve rather subtle reasoning

2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features: In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting unexpected weaknesses in the mechanism

3. Procedures used to provide particular services may be counterintuitive: Typically, a security mechanism is complex (because of 2), and it is not obvious from the statement of a particular requirement that such elaborate measures are needed. It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense

4. Physical (e.g., at what points in a network) and logical (e.g.,at what layer(s) of a protocol stack) placement of various security mechanisms needs to be determined

Computer Security Challenges

5. Security mechanisms typically involve more than a particular algorithm or protocol and also require that participants be in possession of some secret information which raises issues about the creation, distribution, and protection of that secret information

6. Attackers only need to find a single weakness, while the designer must find and eliminate all weaknesses to achieve (perfect) security

7. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs

8. Security requires regular and constant monitoring

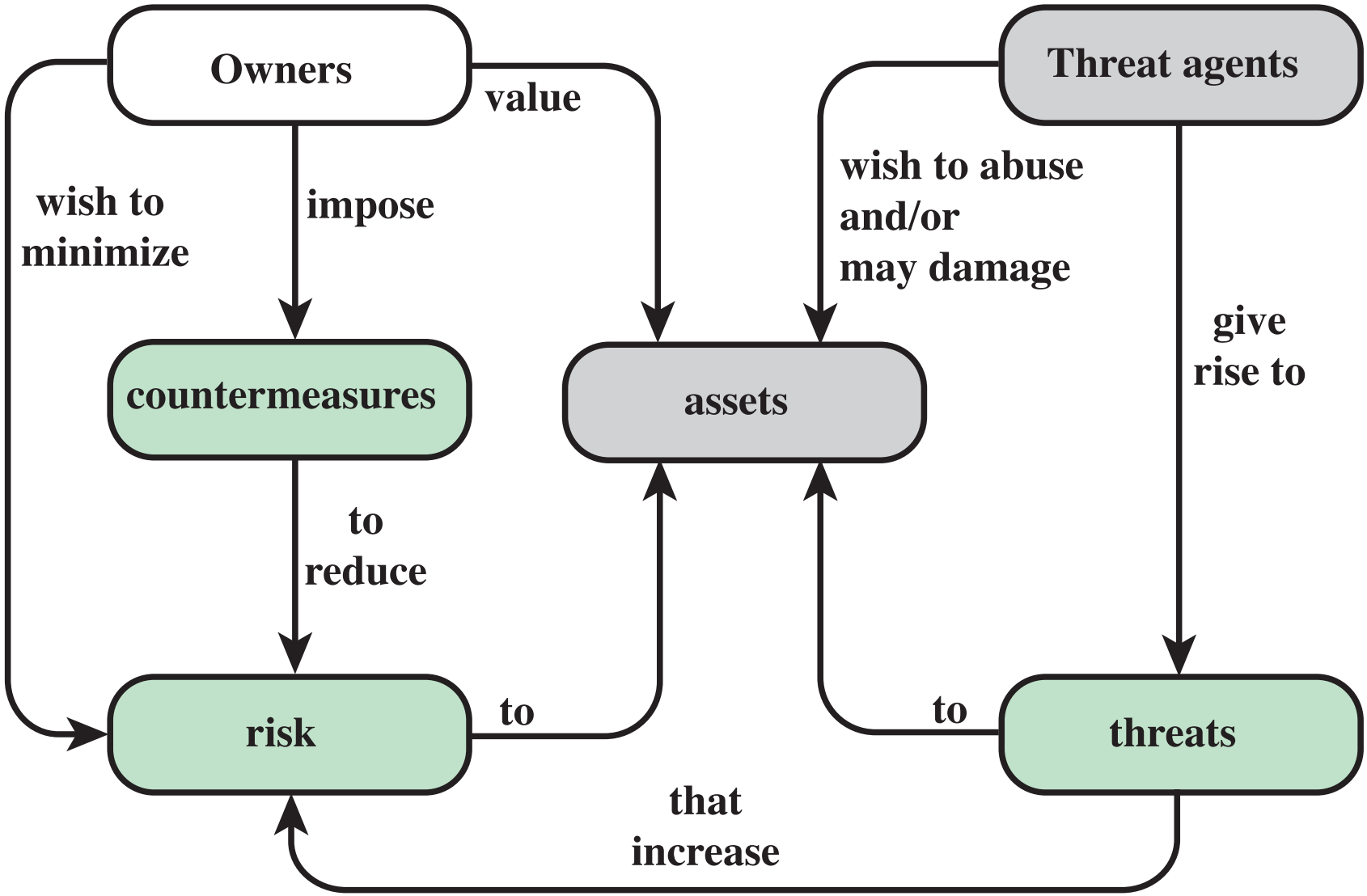
9. Security is still too often an afterthought to be incorporated into a system after the design is complete, rather than being an integral part of the design process

10. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information

A model for Computer Security

- Users and **owners** wish to protect **assets**, or **systems resources**
  - *Hardware*: Including computer systems and other data processing, data storage, and data communications devices
  - *Software*: Including the operating system, system utilities, and applications
  - *Data*: Including files and databases, as well as security-related data, such as password files
  - *Communication facilities and networks*: Local and wide area network communication links, bridges, routers, and so on
- Because of possible **vulnerabilities**, these assets can become
  - *leaky* (loss of confidentiality)
  - *corrupted* (loss of integrity)
  - *unavailable or very slow* (loss of availability)
- **Threats**
  - Can exploit vulnerabilities
  - Represent a potential security harm to an asset
- An **attack** is a threat that is carried out by an **attacker**, or **threat agent**, or **adversary**
  - *Active attack*: An attempt to alter system resources or affect their operation
  - *Passive attack*: An attempt to learn or make use of information from the system that does not affect system resources
  - *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**: actions taken to prevent, detect, recover and minimize **risks** to assets

Security concepts and relationships



Computer Security Terminology

(RFC 2828, Internet Security Glossary, May 2000)

Adversary (threat agent) Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Attack Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

Countermeasure A device or technique that has as its objective the impairment of the operational effectiveness of undesirable or adversarial activity, or the prevention of espionage, sabotage, theft, or unauthorized access to or use of sensitive information or information systems.

Risk A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.

Security Policy A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.

System Resource (Asset) A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Threat Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Index

- Computer Security Concepts
- Threats, Attacks, and Assets
- Security Functional Requirements
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- Computer Security Strategy

Threats, Attacks, and Assets

- We now turn to a more detailed look at threats, attacks, and assets
- First, we look at the types of security threats that must be dealt with
- Then we give some examples of the types of threats that apply to different categories of assets

Threat consequences and attacks

- Unauthorized disclosure: threat to confidentiality
  - *A circumstance or event whereby an entity gains access to data for which the entity is not authorized*
  - Release, interception, or inference of sensitive data, an unauthorized entity circumventing system's security protections (intrusion)
- Deception: threat to integrity
  - *A circumstance or event that may result in an authorized entity receiving false data and believing it to be true*
  - An unauthorized entity posing as an authorized entity (masquerade), data falsification, falsely denying responsibility for an act (repudiation)
- Disruption: threat to integrity and availability
  - *A circumstance or event that interrupts or prevents the correct operation of system services and functions*
  - Disabling a system component (incapacitation), adversely modifying system functions or data (corruption), overload a communication line (obstruction)
- Usurpation: threat to integrity
  - *A circumstance or event that results in control of system services or functions by an unauthorized entity*
  - Theft of service (misappropriation), hacker gaining unauthorized access (misuse)

Threat consequences and attacks (tabular form)

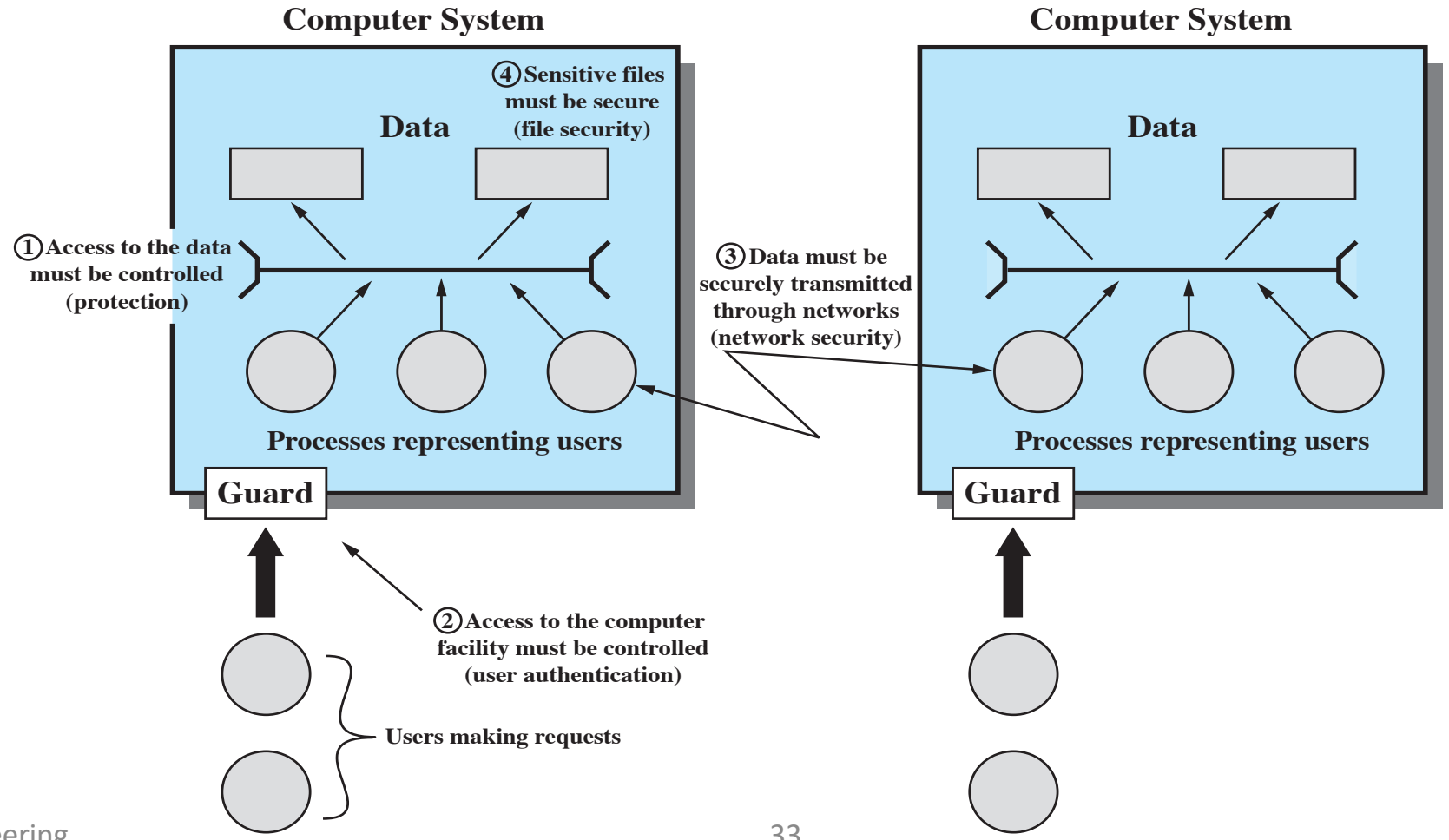
Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	**Exposure:** Sensitive data are directly released to an unauthorized entity. **Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. **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. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.
Deception 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. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.
Disruption 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. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.
Usurpation 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. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security.

Examples of threats to assets

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted DVD or USB drive 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.

The scope of computer security

Security concerns other than physical security (1), include control of access to computers systems (2), safeguarding of data transmitted over communications systems (3), and safeguarding of stored data (4)



Index

- Computer Security Concepts
- Threats, Attacks, and Assets
- Security Functional Requirements
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- Computer Security Strategy

Countermeasures as Functional Requirements

- There are a number of ways of classifying and characterizing the **countermeasures** that may be used to reduce vulnerabilities and deal with threats to system assets
- They can be classified in terms of functional requirements (or *security-related areas*) as done in the **standard FIPS 200** (*Minimum Security Requirements for Federal Information and Information Systems*)
  - This provides us with *a first viewpoint* on the measures that can be taken to deal with security threats and attacks

Security functional requirements

- FIPS 200 enumerates 17 security-related areas, each of them may involve both *computer security technical measures* and *management controls and procedures*
  - **Computer security technical measures** (either HW or SW, or both)
    - Access control; identification & authentication; system & communication protection; system & information integrity
  - **Management controls and procedures**
    - Awareness & training; audit & accountability; certification, accreditation, & security assessments; contingency planning; maintenance; physical & environmental protection; planning; personnel security; risk assessment; systems & services acquisition
  - **Overlapping** computer security technical measures and management controls and procedures
    - Configuration management; incident response; media protection

Security Functional Requirements

Access control: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and training: (i) Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and 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 the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Certification, accreditation, and security assessments: (i) Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Configuration management: (i) Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

Contingency planning: Establish, maintain, and implement plans for emergency response, backup operations, and postdisaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and authentication: Identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Incident response: (i) Establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance: (i) Perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Media protection: (i) Protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

Physical and environmental protection: (i) Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Planning: Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Personnel security: (i) Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Risk assessment: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

Systems and services acquisition: (i) Allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

System and communications protection: (i) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and information integrity: (i) Identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

Some Security Functional Requirements

- Access Control
  - Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise
- Awareness and Training
  - Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, regulation, and policies related to the security of organizational information systems
  - Ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities
- Incident Response
  - Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user-response activities
  - Track, document, and report incidents to appropriate organizational officials and/or authorities

Lessons learned

- FIPS 200 provides a useful summary of the principal areas of concern, both technical and managerial, with respect to computer security
- This course attempts to cover most of these areas

- To achieve effective computer security there is a need to combine technical and managerial approaches

> “If you think technology can solve your security problems, then you don’t understand the problems and you don’t technology”
>
> [Bruce Schneier]

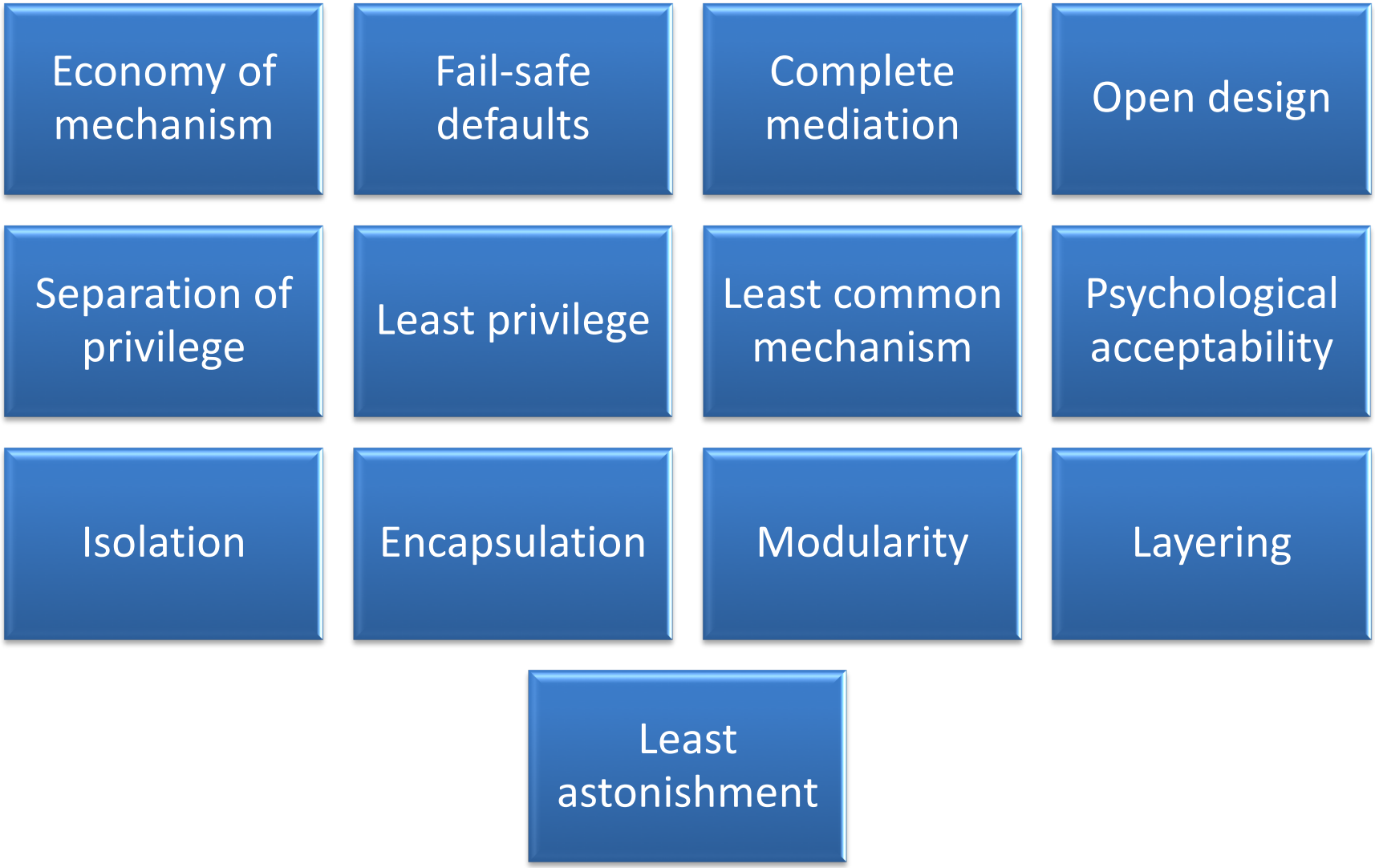
Index

- Computer Security Concepts
- Threats, Attacks, and Assets
- Security Functional Requirements
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- Computer Security Strategy

Fundamental security design principles

- Despite years of research, it is still difficult to design systems that **systematically exclude security flaws** and **prevent all unauthorized actions**
- But good practices for good design have been documented (analogous to software engineering)
- The National Centers of Academic Excellence in Information Assurance/Cyber Defense lists the following as fundamental security design principles
  - Widely agreed security design principles can guide the development of protection mechanisms
  - They provide us with *a second viewpoint* on the measures that can be taken to deal with security threats and attacks

Fundamental security design principles



Fundamental security design principles

- **Economy of mechanism**: the design of security measures should be as simple as possible
  - Simpler to implement and to verify means fewer vulnerabilities
- **Fail-safe default**: access decisions should be based on permissions (the default is lack of access)
  - A mechanism that gives explicit permission tends to fail by refusing permission, a safe situation that can be quickly detected
- **Complete mediation**: every access should be checked against an access control mechanism
  - Systems should not rely on access decisions retrieved from a cache
- **Open design**: the design should be open rather than secret
  - For example, although encryption keys must be secret, encryption algorithms should be open to public scrutiny: The algorithms can then be reviewed by many experts, and users can therefore have high confidence in them

Fundamental security design principles

- **Separation of privilege**: multiple privileges should be needed to achieve access or complete a task
  - For example, multifactor user authentication requires the use of multiple techniques, such as a password and a smart card, to authorize a user
- **Least privilege**: every user (process) should have the least privilege needed to perform a task
  - There is also a temporal aspect to the least privilege principle
  - For example, system programs or administrators who have special privileges should have those privileges only when necessary: when they are doing ordinary activities the privileges should be downgraded
- **Least common mechanism**: the design should minimize the functions shared by different users, thus reducing the number of unintended communication paths
- **Psychological acceptability**: security procedures must reflect the user's mental model of protection
  - Security mechanisms should not interfere improperly with users' work

Fundamental security design principles

- **Isolation** applies in three contexts:
  - Public access systems should be isolated from critical resources (data, processes, etc.) to prevent disclosure or tampering
  - Processes and files of individual users should be isolated from one another (except when desired)
  - Security mechanisms should be isolated (i.e., access to those mechanisms should be prevented)
- **Encapsulation**: a collection of procedures and data objects are encapsulated in a domain of its own so that the internal structure of a data object is accessible only to the procedures of the protected subsystem and the procedures may be called only at designated domain entry points (similar to object-orientation)

Fundamental security design principles

- **Modularity**: refers to
  - security functions developed as separate, protected modules
    - For example, numerous protocols and applications make use of cryptographic functions; rather than implementing such functions in each protocol or application, a more secure design is to develope a common cryptographic module that can be invoked by numerous protocols and applications
  - mechanisms design and implementation rely on a modular architecture so that individual parts of the security design can be upgraded without the requirement to modify the entire system
- **Layering**: use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems
  - Thus, the failure or circumvention of any individual protection approach will not leave the system unprotected (defense in depth)
- **Least astonishment**: a program or interface should always respond in a way that is least likely to astonish a user

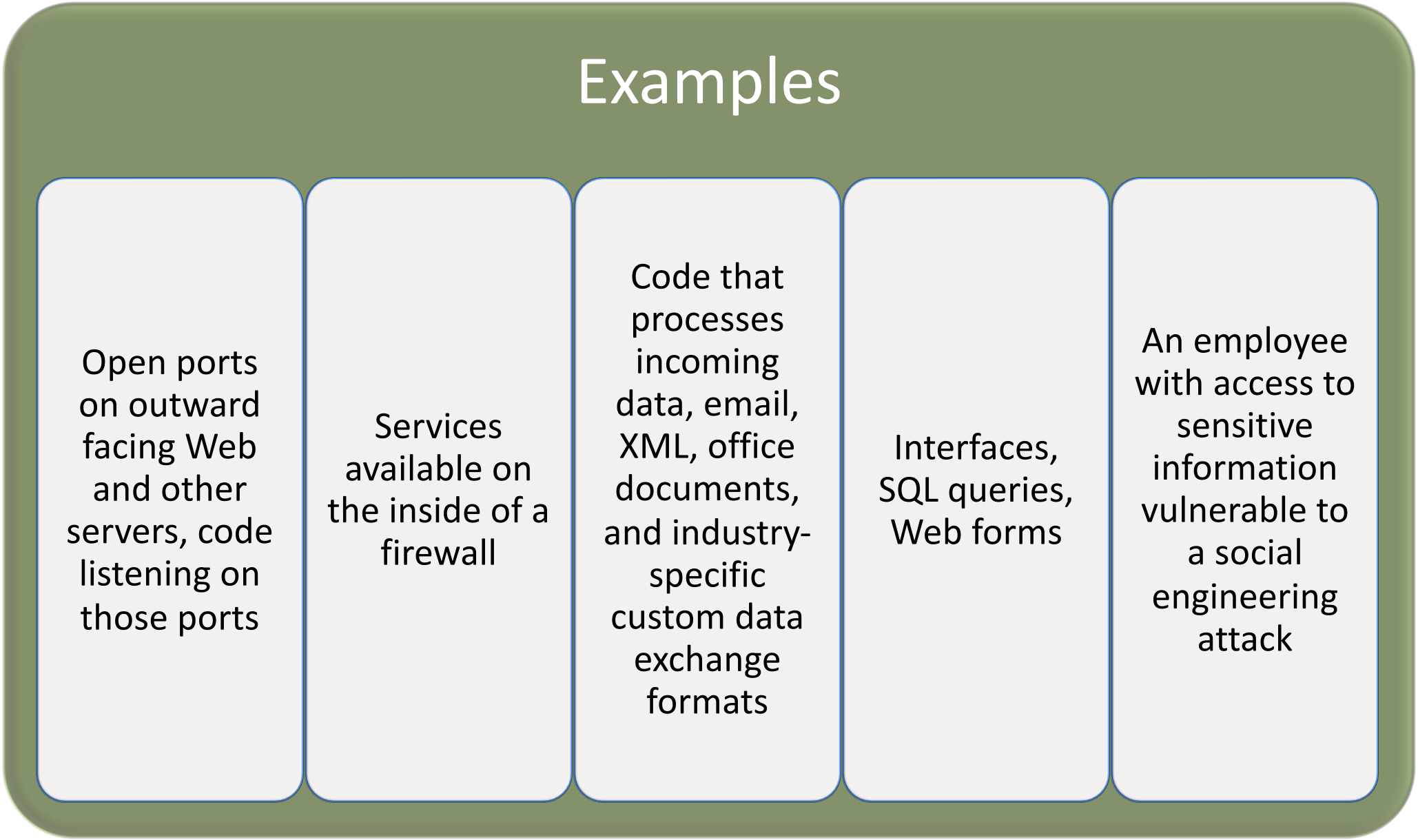
Index

- Computer Security Concepts
- Threats, Attacks, and Assets
- Security Functional Requirements
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- Computer Security Strategy

Attack surfaces and attack trees

- We elaborate on two concepts that are useful in evaluating and classifying threats:
  - attack surfaces
  - attack trees
- This provides us with *a third viewpoint* on the measures that can be taken to deal with security threats and attacks

Some reachable and exploitable vulnerabilities in a system



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, program utility, operating system

Particular focus is Web server software

Human Attack Surface

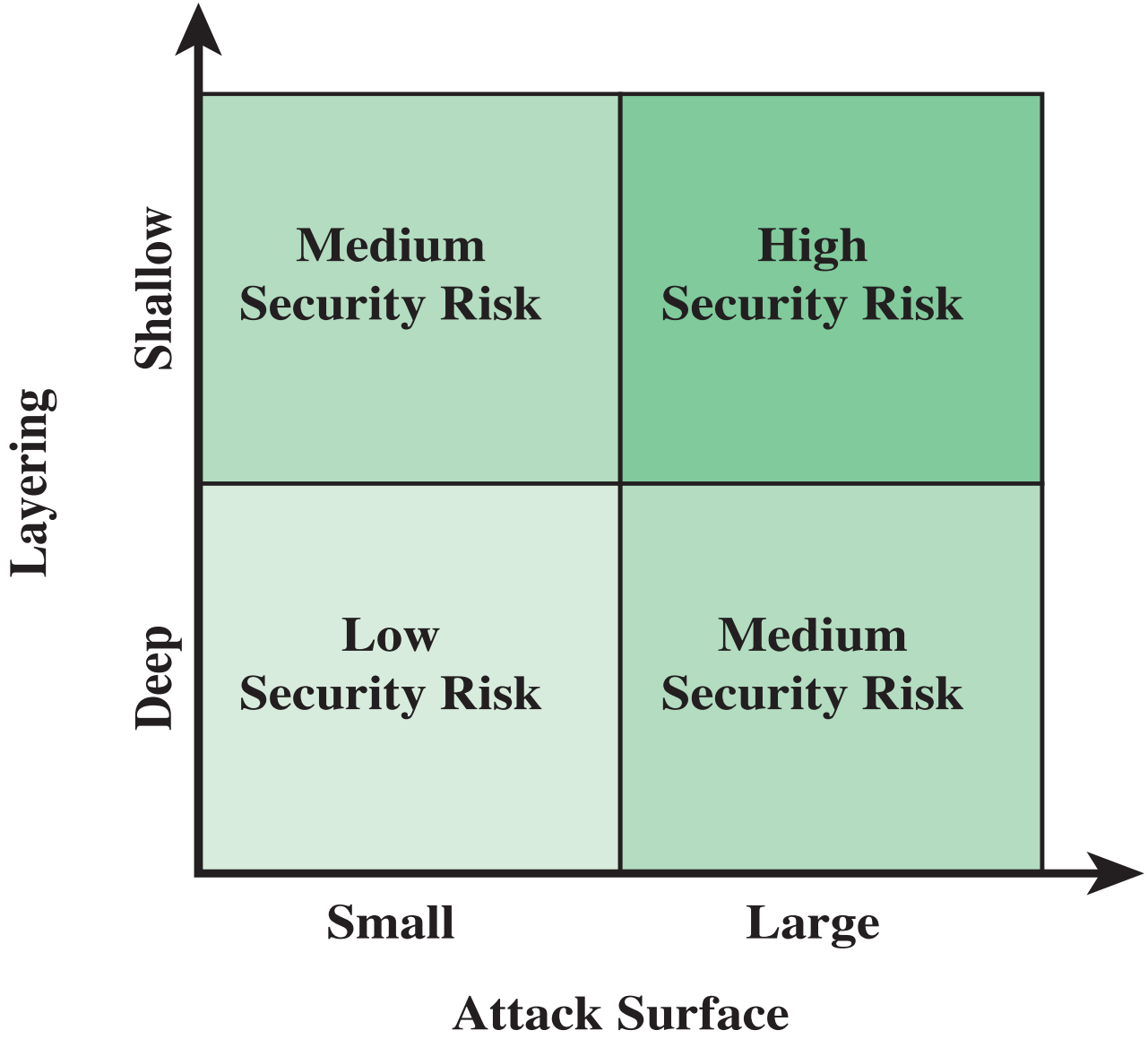
Vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders

Attack surface analysis

- An **analysis of an attack surface** is useful for assessing the scale and severity of threats to a system
- Once an attack surface is defined, designers may be able to find ways to **make the surface smaller**

Defense in Depth and Attack Surface

Use of layering (multiple, overlapping protection approaches), or defense in depth, and attack surface reduction complement each other in mitigating security risk



Attack tree

- A branching, hierarchical **data structure** that represents a set of potential vulnerabilities
- Objective: to effectively exploit the info available on *attack patterns*
  - Security advisories, published on CERT (*Computer Emergency Response Team*) or similar forums, have enabled the development of a body of knowledge about both general attack strategies and specific attack patterns
  - Security analysts can use attack trees to guide both the design of systems and applications, and the choice and strength of countermeasures

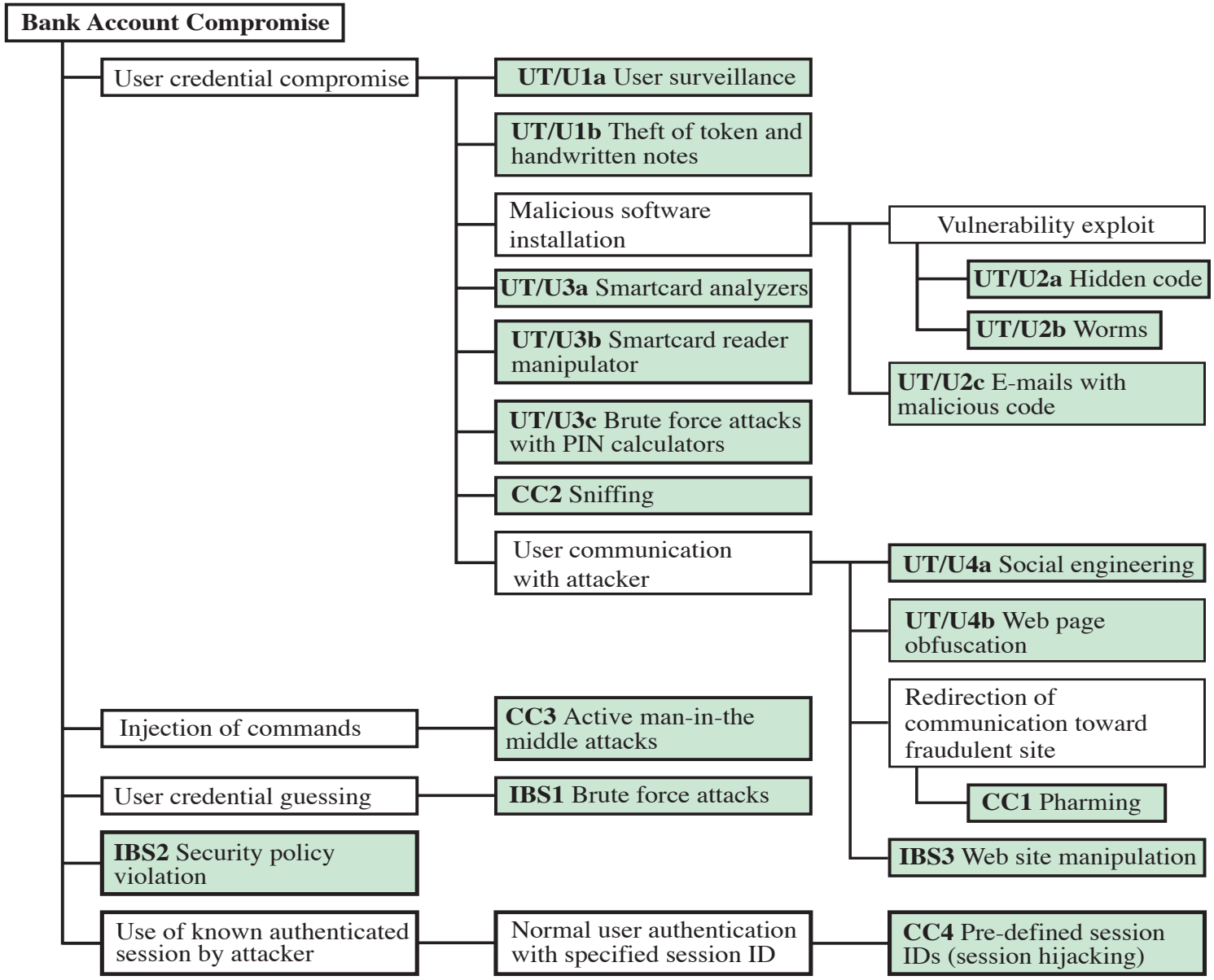
Attack tree

- The goal of the attack (i.e. the security incident) is represented as the root node of the tree
- The ways that an attacker could reach that goal are iteratively and incrementally represented as branches of the tree
- Each subnode defines a subgoal, and each subgoal may have its own set of further subgoals, etc
- The final nodes on the paths outward from the root, i.e., the leaf nodes, represent different ways to initiate an attack
- Each node other than a leaf is either an AND-node or an OR-node
  - To achieve the goal represented by an AND-node, the subgoals represented by all of that node's subnodes must be achieved
  - and for an OR-node, at least one of the subgoals must be achieved
- Branches can be labeled with values representing difficulty, cost, or other attack attributes, so that alternative attacks can be compared

An attack tree for an Internet banking authentication application

- The root of the tree is the objective of the attacker, which is to compromise a user's account
- The **green boxes** on the tree are the leaf nodes, which represent events that constitute the attacks
- The **white boxes** are categories which consist of one or more specific attack events (leaf nodes)
- All the nodes other than leaf nodes are **OR-nodes**
- The analysis used to generate this tree considered the **three components involved in authentication**:
  - **User terminal and user (UT/U):** These attacks target the user equipment, including the tokens that may be involved, such as smartcards or other password generators, and the actions of the user
  - **Communications channel (CC):** These attacks focus on communication links
  - **Internet banking server (IBS):** These are offline attacks against the servers that host the Internet banking application

An attack tree for an Internet banking authentication application



An attack tree for an Internet banking authentication application

Five overall attack strategies can be identified, each of which exploits one or more of the three components

- **User credential compromise**: e.g. monitoring a user's action to observe a PIN or other credential, thieving the user's token or handwritten notes, embedding malicious software to compromise the user's login and password, hacking the smartcard, using a brute force approach to guess the PIN, sniffing credential information via the communication channel
- **Injection of commands**: e.g. intercepting communication between the UT and the IBS, impersonating the valid user to gain access to the banking system
- **User credential guessing**: e.g. mounting brute force attacks by sending random usernames and passwords
- **Security policy violation**: e.g. by violating the bank's security policy in combination with weak access control and logging mechanisms, an employee may cause an internal security incident and expose a customer's account
- **Use of known authenticated session**: e.g. forcing the user to connect to the IBS with a preset session ID that the attacker can utilize to spoof the user's identity

Index

- Computer Security Concepts
- Threats, Attacks, and Assets
- Security Functional Requirements
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- Computer Security Strategy

Computer security strategy

A comprehensive strategy for providing security involves three aspects

- Specification/policy: what the security scheme is supposed to do?
- Implementation/mechanisms: how to enforce it
- Correctness/assurance: does it really work?

Specification/policy

A (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

- In developing a security policy, a security manager needs to consider the following factors:
  - The value of the assets being protected
  - The vulnerabilities of the system
  - Potential threats and the likelihood of attacks

  and trade-offs
  - *Ease of use vs security benefits* (e.g. access control mechanisms require users to remember passwords, firewalls and other network security measures may reduce available transmission capacity or slow response time, virus-checking software reduces available processing power)
  - *Cost of security vs cost of failure and recovery*: direct monetary costs in implementing and maintaining security measures must be balanced against the cost of security failure and recovery if certain security measures are lacking

A *business decision*, possibly influenced by legal requirements

Implementation/mechanisms

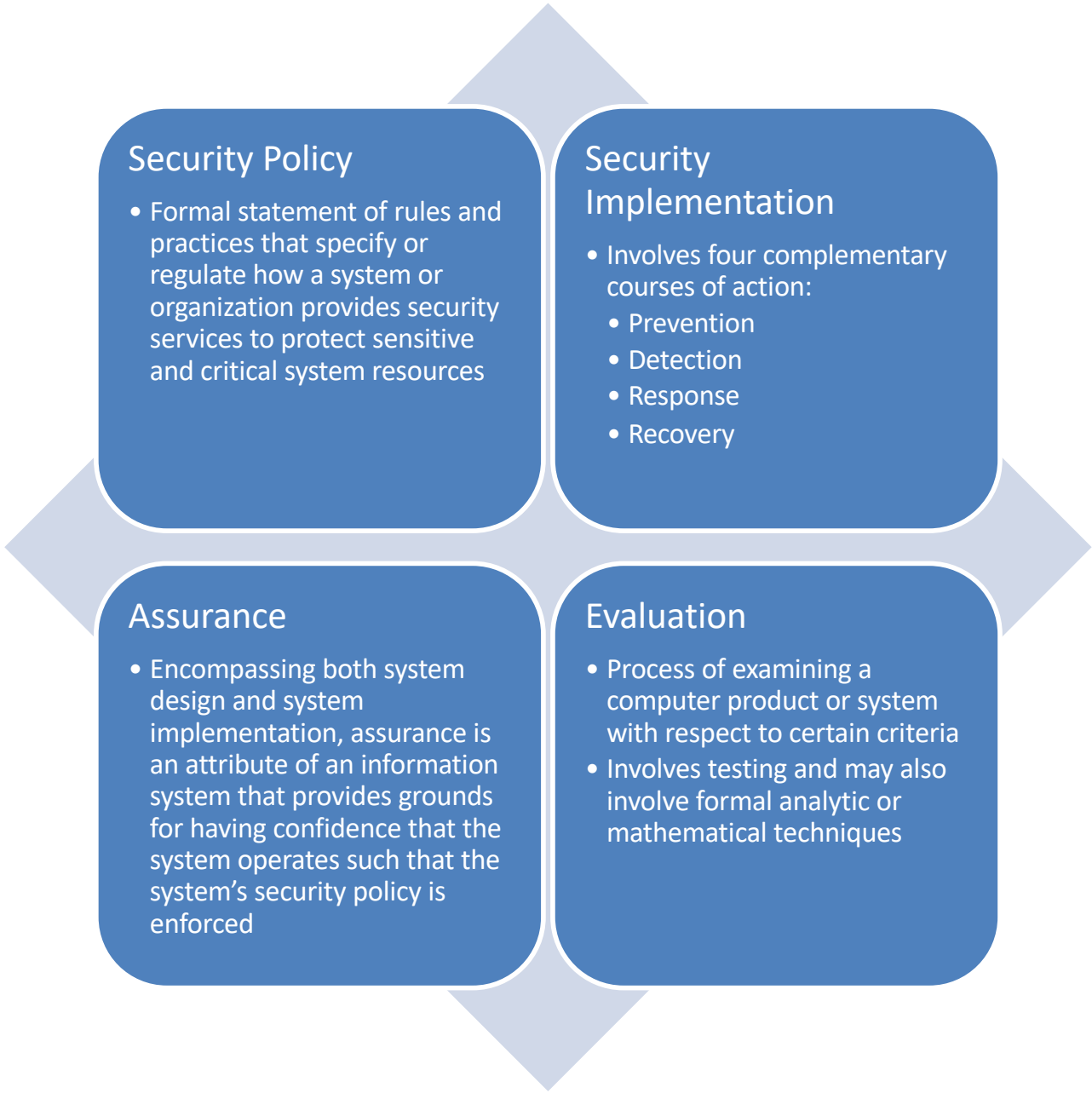
Security implementation involves four complementary courses of action

- Prevention: an ideal security scheme is one in which no attack is successful; sometimes prevention is a reasonable goal
  - E.g. attacks on confidentiality prevented by transmission of encrypted data
- Detection: in a number of cases, absolute protection is not feasible, but it is practical to detect security attacks
  - E.g. intrusion detection or detection of denial of service attacks
- Response: the system may be able to respond in such a way as to halt a detected attack and prevent further damage
- Recovery: e.g. if data integrity is compromised, a prior, correct copy of the data can be reloaded

Correctness/assurance

- *Consumers* of computer security services and mechanisms (e.g., system managers, vendors, customers, and end users) want to feel that the security infrastructure of their systems meet security requirements and enforce security policies
  - These considerations bring us to the concepts of assurance and evaluation
- **Assurance** is 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
  - This encompasses both system design and system implementation
  - Assurance is expressed as a degree of confidence, as the state of the art in proving correctness of designs and implementations is such that it is not possible to provide absolute proof
- **Evaluation** is the process of examining a computer product or system with respect to certain **criteria**
  - Involves testing and, possibly, formal analytic or mathematical techniques
  - The goal is developing evaluation criteria that can be applied to any security system (encompassing security services and mechanisms) and that are broadly supported for making product comparisons

Computer Security Strategy



Standards

- Standards have been developed to cover management practices and the overall architecture of security mechanisms and services
- The most important organizations promoting standards are:
  - **National Institute of Standards and Technology (NIST)**
    - NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private sector innovation
  - **Internet Society (ISOC)**
    - ISOC is a professional membership society addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards
  - **ITU Telecommunication Standardization Sector (ITU-T)**
    - ITU (International Telecommunication Union) is a United Nations agency in which governments and the private sector coordinate global telecom networks and services
    - ITU-T is one of the three sectors of the ITU, its mission is the production of standards covering all fields of telecommunications
  - **International Organization for Standardization (ISO)**
    - ISO is a nongovernmental organization whose work results in international agreements that are published as International Standards

Summary

- Computer Security Concepts
  - A Definition of Computer Security
  - The Challenges of Computer Security
  - A Model for Computer Security
- 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
- Standards