COMPUTER SECURITY

PRINCIPLES AND PRACTICE

SECOND EDITION

William Stallings | Lawrie Brown

Chapter 1

Overview

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

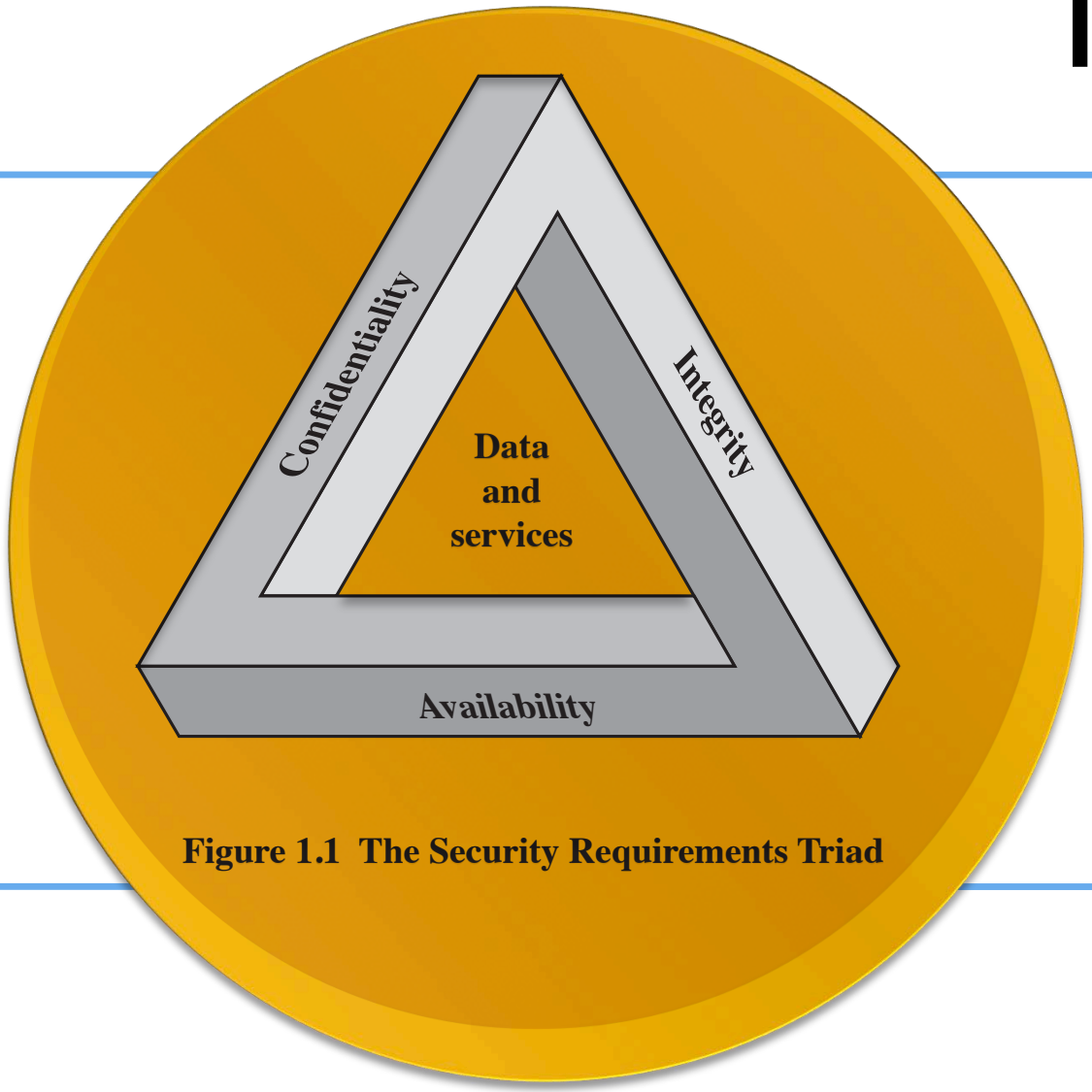


Figure 1.1 The Security Requirements Triad

- **Confidentiality**
  - data confidentiality
  - privacy
- **Integrity**
  - data integrity
  - system integrity
- **Availability**

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

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

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; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the 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.

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 or regulate how a system or organization provides security services 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, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component--hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

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. That is, a threat is a possible danger that might exploit a vulnerability.

Vulnerability
A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

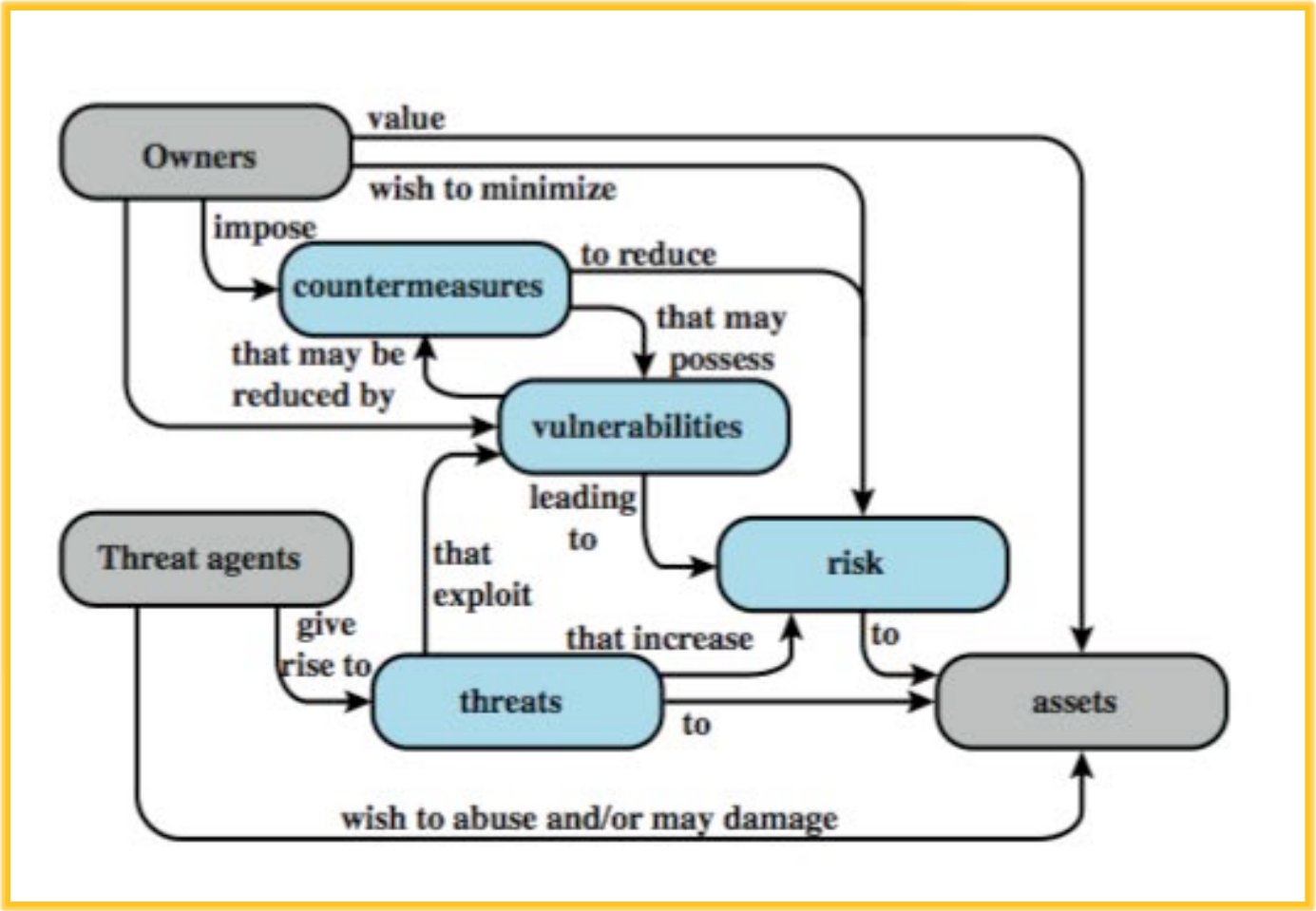
Table 1.1

Computer Security Terminology

RFC 2828, *Internet Security Glossary,*

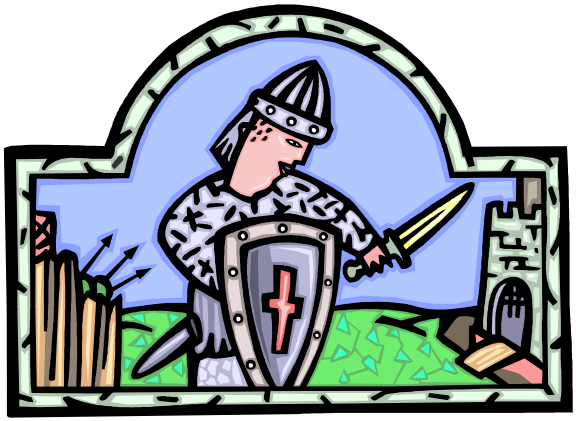
May 2000

Figure 1.2
Security Concepts and Relationships



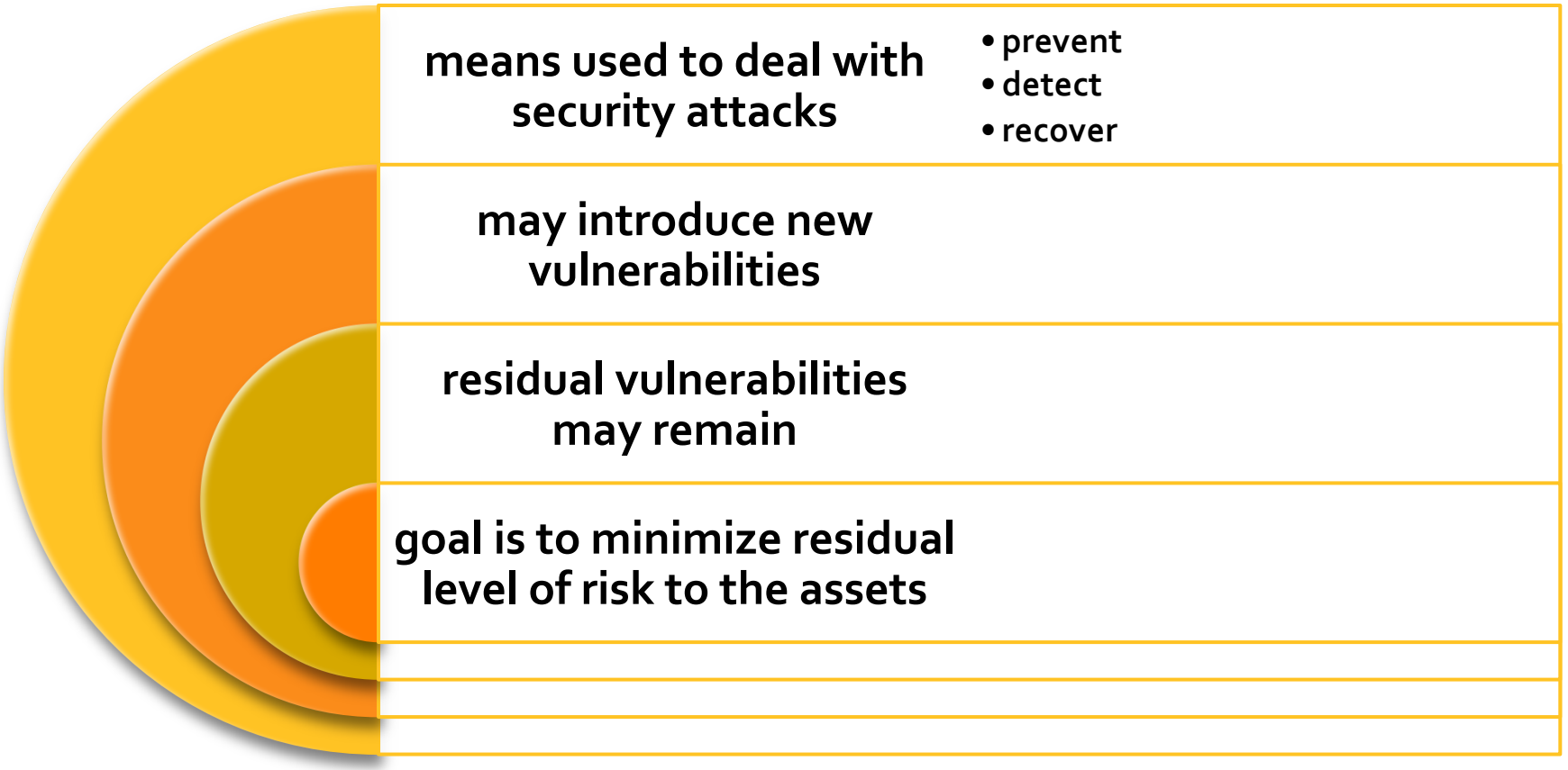
Vulnerabilities, Threats and Attacks

- 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 – 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 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.

Table 1.2

Threat Consequences

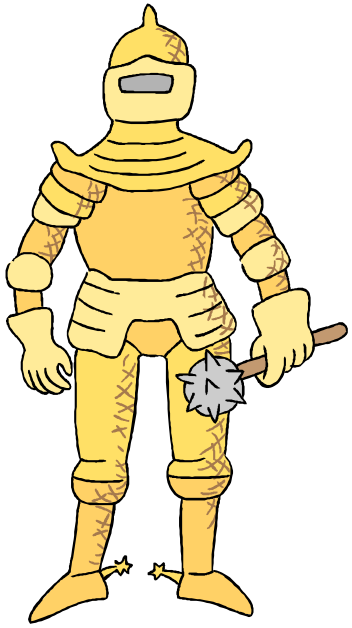


Figure 1.3
Scope of Computer Security

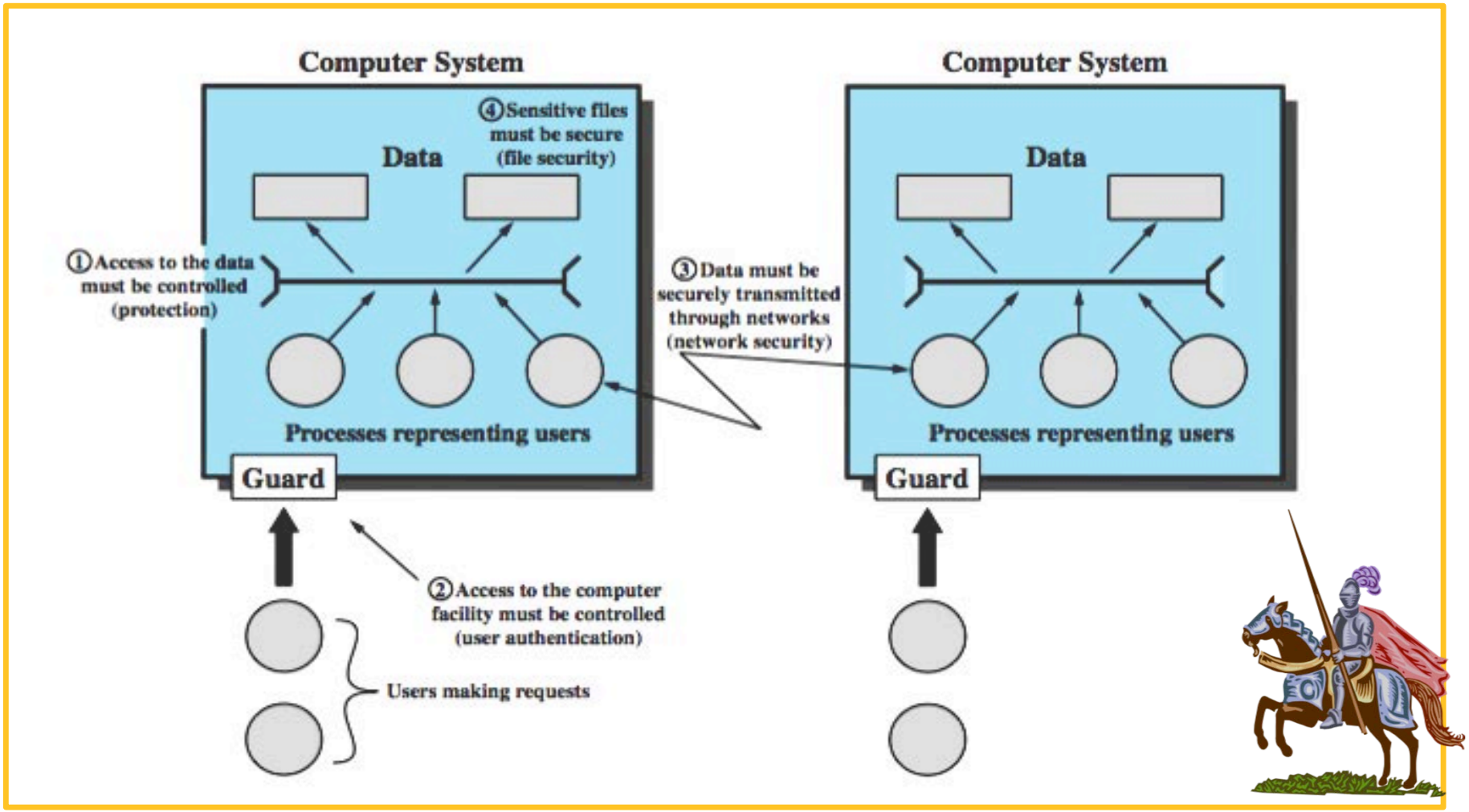
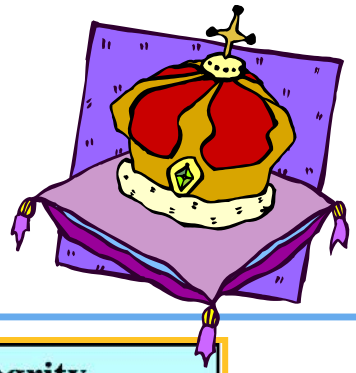
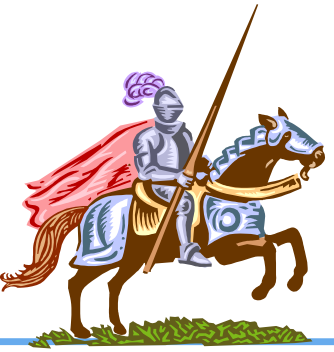


Table 1.3
Computer and Network Assets
Examples of Threats



	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		
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	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.

Table 1.3 Computer and Network Assets, with Examples of Threats.

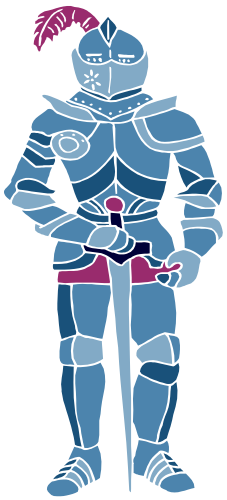


Passive and Active Attacks

- *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
  - four categories:
    - masquerade
    - replay
    - modification of messages
    - denial of service

Table 1.4
(FIPS PUB 200)

Security 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.

Security Functional Requirements

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

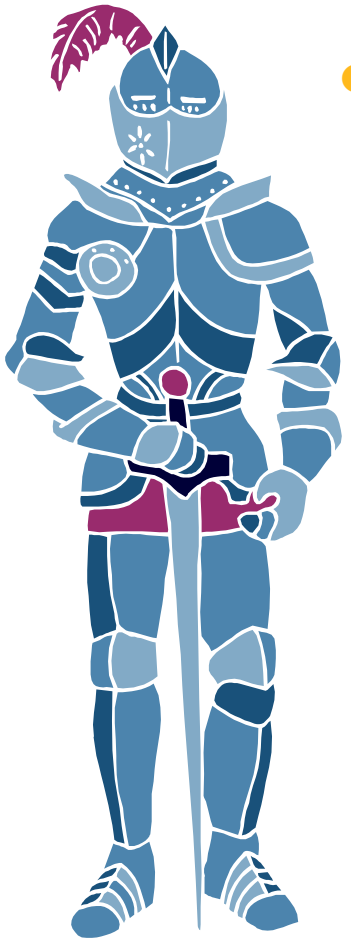
Security Architecture For Open Systems

- ITU-T Recommendation X.800, *Security Architecture for OSI*
  - systematic way of defining the requirements for security and characterizing the approaches to satisfying them
  - was developed as an international standard
  - focuses on:
    - security attacks – action that compromises the security of information owned by an organization
    - security mechanism – designed to detect, prevent, or recover from a security attack
    - security service – intended to counter security attacks

Security Services

X.800

- defines a security service as a service that is provided by a protocol layer of communicating open systems and ensures adequate security of the systems or of data transfers



RFC 2828

- defines a security service as a processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms

Table 1.5

Security Services

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block.

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

AVAILABILITY

Ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to events impacting the network. Disaster recovery solutions are included in this category.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

Source: From X.800, Security Architecture for OSI

- Data Origin Authentication
  - provides for the corroboration of the source of a data unit
  - does not provide protection against the duplication or modification of data units
  - this type of service supports applications like email where there are no prior interactions between the communicating entities

- concerned with assuring that a communication is from the source that it claims to be from
- must assure that the connection is not interfered with by a third party masquerading as one of the two legitimate parties

- Peer Entity Authentication
  - provides for the corroboration of the identity of a peer entity in an association
  - provided for use at the establishment of, or at times during the data transfer phase of, a connection
  - attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection

Access Control Service

Nonrepudiation Service

- the ability to limit and control the access to host systems and applications via communications links
- each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual

- prevents either sender or receiver from denying a transmitted message
- receiver can prove that the alleged sender in fact sent the message
- the sender can prove that the alleged receiver in fact received the message

- the protection of transmitted data from passive attacks
- the broadest service protects all user data transmitted between two users over a period of time
- connection confidentiality
  - the protection of all user data on a connection
- protects the traffic flow from analysis
  - this requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility
- connectionless confidentiality
  - protection of all user data in a single data block
- selective-field confidentiality
  - confidentiality of selected fields within the user data on a connection or a single data block
- traffic-flow confidentiality
  - protection of the information that might be derived from observation of traffic flows

- can apply to a stream of messages, a single message, or selected fields within a message
- a connectionless integrity service generally provides protection against message modification only
- a connection-oriented integrity service assures that messages are received as sent, with no duplication, insertion modification, reordering, or replays
  - destruction of data is also covered under this service
  - addresses both message stream modification and denial of service
- need to make a distinction between the service with and without recovery
  - concerned with detection rather than prevention
  - the incorporation of automated recovery mechanisms is the more attractive alternative

- a service that protects a system to ensure its availability
  - defined as the property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications of the system

- a variety of attacks can result in the loss of or reduction in availability
  - some of these attacks are amenable to authentication and encryption
  - some attacks require a physical action to prevent or recover from loss of availability

- X.800 treats availability as a property to be associated with various security services

- addresses the security concerns raised by denial-of-service attacks

- depends on proper management and control of system resources

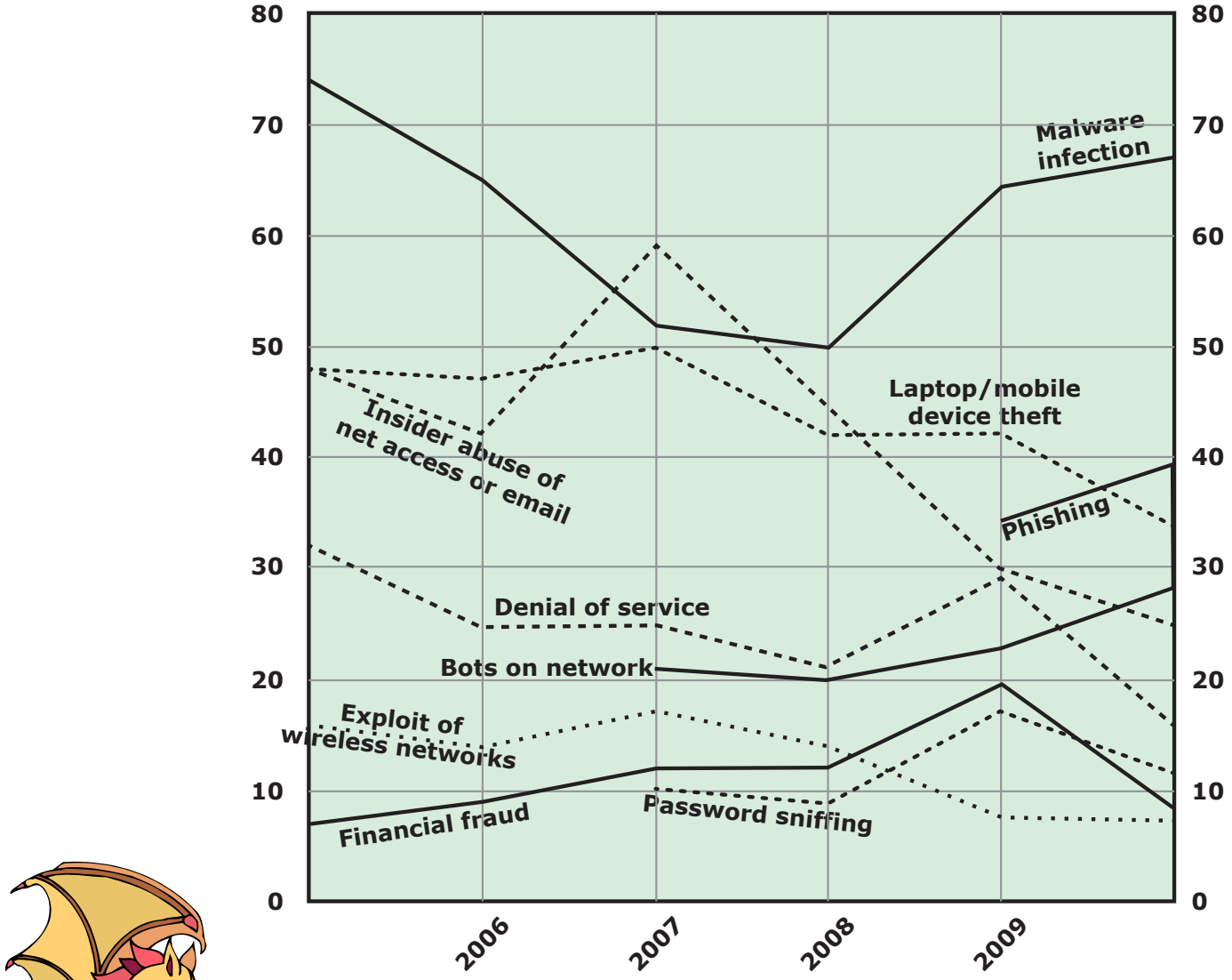
SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**Security Audit Trail** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.	**Security Recovery** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.
Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.	
Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.	
Notarization The use of a trusted third party to assure certain properties of a data exchange.	

Table 1.6

X.800 Security Mechanisms

Figure 1.4

Security Trends



Source: Computer Security Institute 2010/2011 Computer Crime and Security Survey

Figure 1.4 Types of Attacks Experienced (by percent of respondents)

Source: Computer Security Institute 2010/2011 Computer Crime and Security Survey

Figure 1.5 Security Technologies Used

Figure 1.5

Security Technologies Used

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?

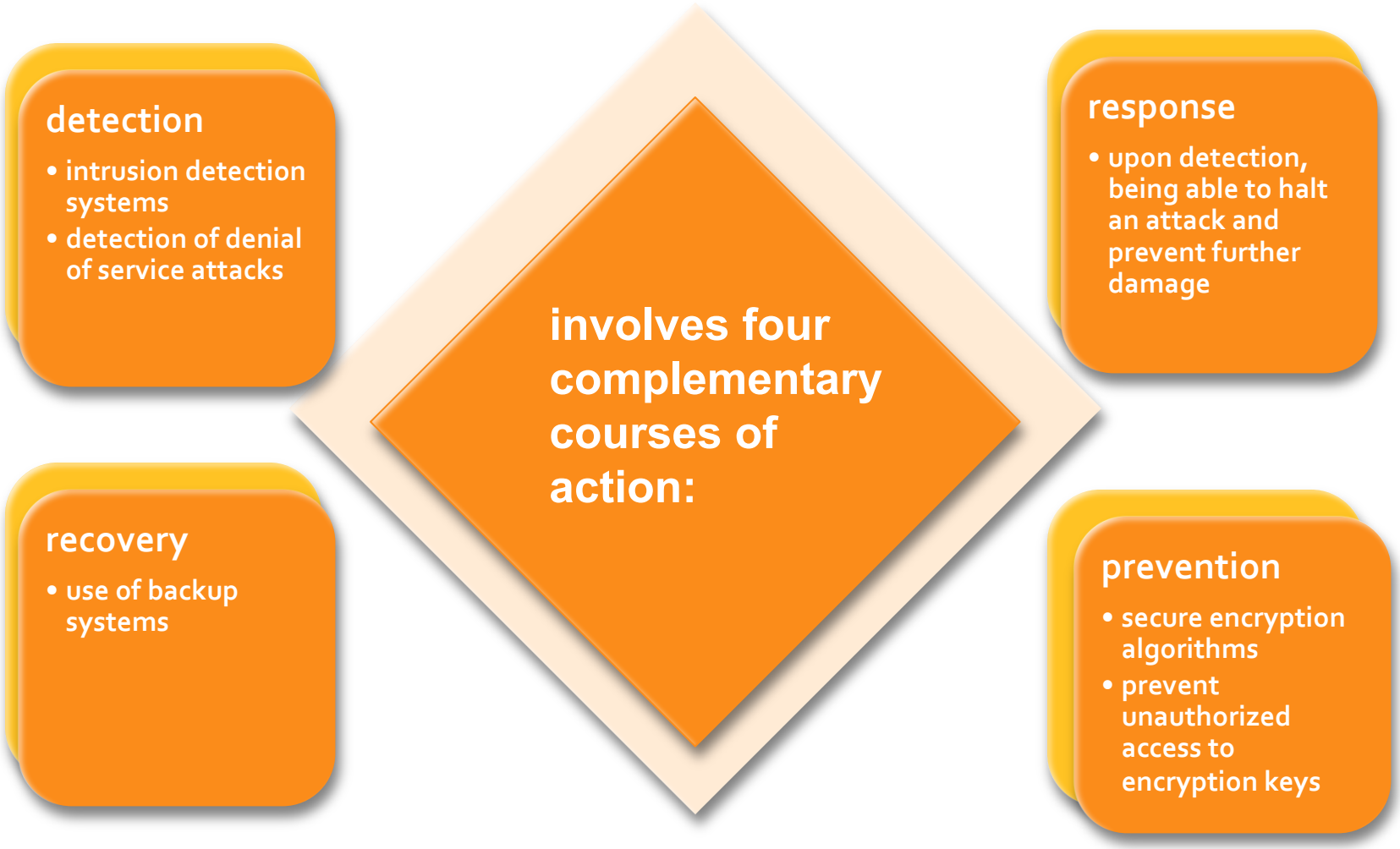
Security Policy

- 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

- factors to consider:
  - value of the assets being protected
  - vulnerabilities of the system
  - potential threats and the likelihood of attacks

- trade-offs to consider:
  - ease of use versus security
  - cost of security versus cost of failure and recovery

Security Implementation



Assurance and Evaluation

- **assurance**
  - **the *degree* of confidence one has that the security measures work as intended to protect the system and the information it processes**
  - **encompasses both system design and system implementation**
- **evaluation**
  - **process of examining a computer product or system with respect to certain criteria**
  - **involves testing and formal analytic or mathematical techniques**

Summary

- security concepts
  - CIA triad
    - confidentiality – preserving the disclosure of information
    - integrity – guarding against modification or destruction of information
    - availability – ensuring timely and reliable access to information
- terminology – table 1.1
  - threats – exploits vulnerabilities
  - attack – a threat carried out
  - countermeasure – means to deal with a security attack
  - assets – hardware, software, data, communication lines, networks
- security architecture
  - security services – enhances the security of systems and information transfers, table 1.5
  - security mechanisms – mechanisms designed to detect, prevent, or recover from a security attack, table 1.6
  - security attack – any action that compromises the security of information owned by an organization
- security trends
  - figure 1.4
- security strategy
  - policy, implementation, assurance and evaluation
- functional requirements
  - table 1.4