SLIIT
Discover Your Future

IE2022 – Introduction to Cyber Security

Lecture - 01

Introduction

Mr. Amila Senarathne

SLIIT
FACULTY OF COMPUTING

Lecture 1: Introduction to Cyber Security

Objective:

- Describe the formal definition of Computer Security
- Describe Confidentiality, Integrity, and Availability as the key security requirements
- Computer Security Model and Strategy
- Describe the security threats and attacks types

Recommended Texts

W. Stallings and L. Brown, “Computer Security, Principles and Practice, 2nd edition, Pearson, 2012, Chapter 1.

Supplementary text

Charles P. Pfleeger and Shari L. Pfleeger, Security in Computing (3rd edition). Prentice-Hall. 2003. ISBN: 0-13-035548-8.

Computer Security

Definition (NIST Computer Security Handbook)

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*).

Key objectives of Computer Security:

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

Information Security (InfoSec)

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

(Source : NIST Glossary of Key Information Security Terms)

Computer Security Objectives

1) **Confidentiality** (**C**).

This term covers two related concepts.

- Data confidentiality. Assures that confidential information is not made available or disclosed to unauthorized individuals.
- Privacy. Assures that the owners have control on:
  - What information related to them may be collected and stored,
  - By whom and to whom that information may be disclosed.

NIST’s Requirement: Preserve authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Loss of confidentiality means unauthorized disclosure of information.

Objectives (cont.)

2) **Integrity** (**I**).

This term covers two related concepts.

- Data integrity: Information and programs are changed only in a specified and authorized manner.
- System integrity: A system performs its intended function
  - in an unimpaired manner, and
  - free from deliberate or inadvertent unauthorized manipulation of the system.

Requirement: Guard against improper information modification or destruction, including ensuring information nonrepudiation authenticity.

Loss of Integrity means unauthorized modification or destruction of information.

Objectives (cont.)

3) **Availability** (**A**).

Systems work promptly and service is not denied to authorized users.

NIST’s requirement: Ensuring timely and reliable access and use of information.

Loss of Availability means disruption to the authorized users in accessing or use of information.

Figure from Stallings & Brown textbook

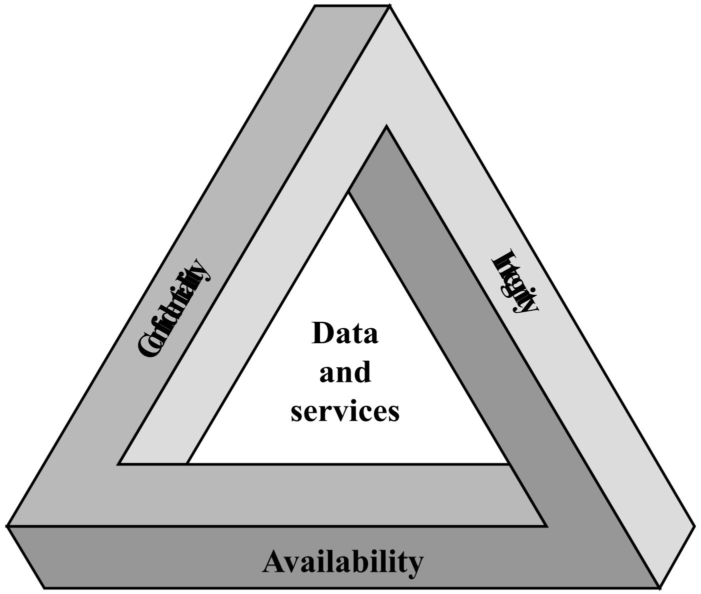


Figure 1.1 The Security Requirements Triad

Additional Objectives

4) **Authenticity**: Able to verify that

- the users are who they claim they are, and
- the system receives data from a trusted source.

NIST includes authenticity as part of Integrity

5) **Accountability**: Able to trace back the actions performed by an entity to that entity.

Accountability supports: nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, after-action recovery and legal action.

Read the examples of C-I-A in the textbook (Stallings & Brown)

Computer Security Model (RFC 2828)

1) **System Resource** or asset that needs to be protected

Hardware: e.g., Computer System, data storage, communication devices.

Software: e.g., operating systems, program utilities and applications.

Data: e.g., data and password files, databases.

Communication facilities and networks: e.g., LAN, WAN, routers, etc.

2) **Vulnerabilities** of system resources

Definition: A flaw or weaknesses in a system’s design, implementation, or operation and management that could be exploited to violate the system’s security policy.

When the resource is corrupted → violate Integrity

When the resource is leaky → violate Confidentiality

When the resource is unavailable → violate Availability

Computer Security Model

3) **Threat** is a possible danger that might exploit a vulnerability.

It represents a potential harm to the system resource.

4) **Attack** is a threat that is carried out (threat action)

Two attack types:

- Active attack: An act that has negative effects on system resources
- Passive attack: An act to make use of system information but it does not affect the system

The origin of an attack:

- Inside attack is carried out by an entity inside the security perimeter.
- Outside attack is performed by an unauthorized users.

Computer Security Model (cont.)

5) **Adversary** is an entity that carried out an attack

- A threat agent or an attacker.

6) **Countermeasure** is any means taken

- to address an attack,
- to prevent an attack from being successful,
- to detect the attack if the attack is successful, and
- to recover from the damage due to the attack.

7) **Risk** is the expected loss due to a particular attack.

- Examples?

Exploits

An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized).

Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service (DoS or related DDoS) attack.

Used as a verb, exploit refers to the act of successfully making such an attack (make use of a vulnerability).

Vulnerability Assessment

A vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in Information systems, applications and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately.

Penetration Testing

Penetration testing (also called pen testing or ethical hacking) is the practice of testing a Information system, network or web application to find security vulnerabilities that an attacker could exploit. The process involves gathering information about the target before the test, identifying possible entry points, attempting to break in either virtually or for real and reporting back the findings.

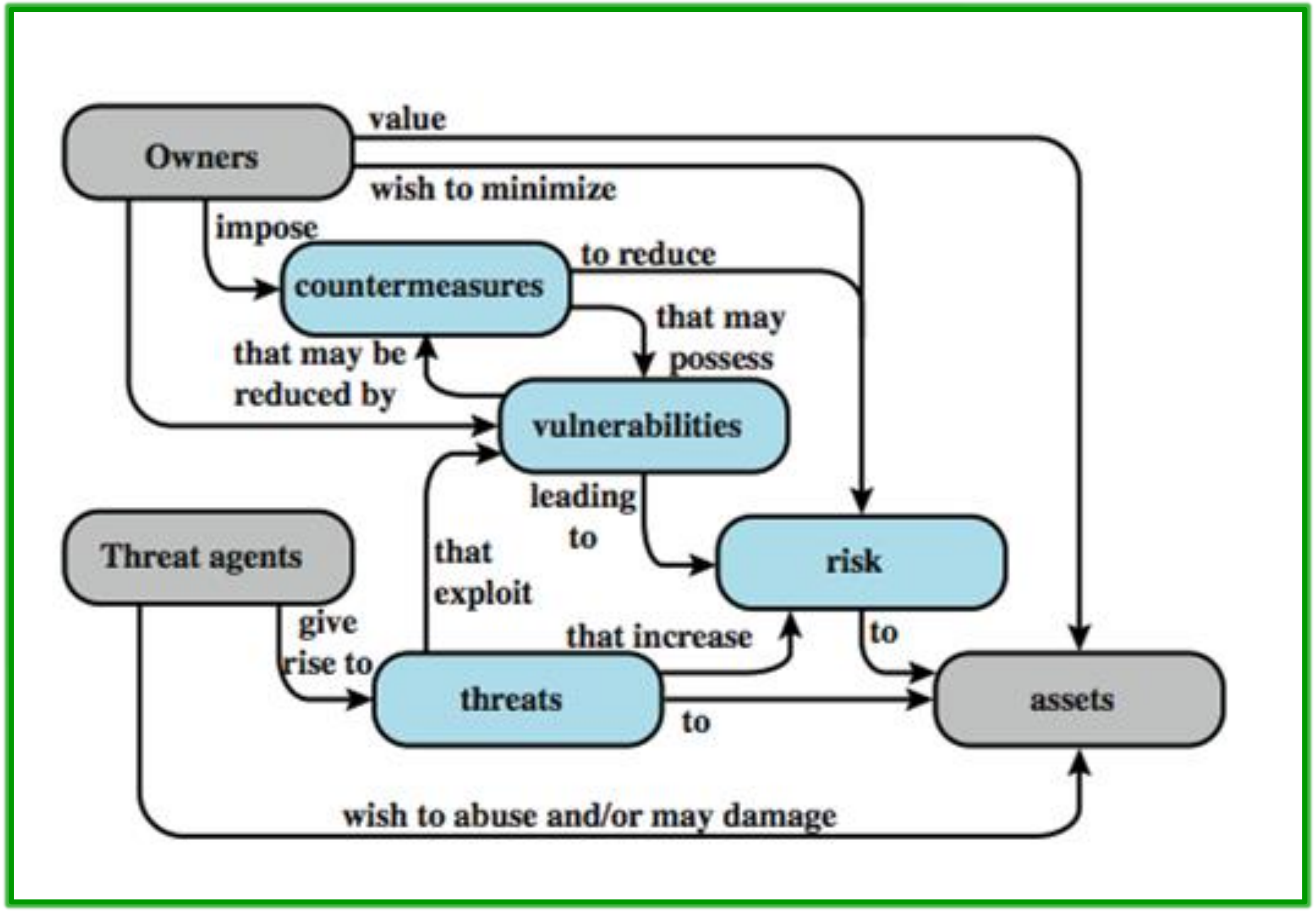
Penetration testing can be automated with software applications or performed manually.

Goal of Penetration Testing

- Identify weak spots in an organization's security posture
- Measure the compliance of its security policy
- Test the staff's awareness of security issues
- Determine whether and how the organization would be subject to security disasters.

Computer Security Model

Figure from Stallings
& Brown textbook



Threats and Attacks

Four kinds of threats and their types of attacks (RFC 2828)

1) **Unauthorized disclosure**: a threat to system confidentiality

Types of Attacks:

Exposure. The attacker obtains unauthorized knowledge of sensitive data.

Interception. The attacker gain access to data being transmitted

- A common attack in communication network

Inference. The attacker gains information from analyzing the pattern of traffic in a network

Intrusion. The attacker gains unauthorized access to data

- Probably after breaking the system's access control protection

Threats and Attacks (cont.)

2) **Deception**: a threat to system or data integrity

Types of Attacks:

Masquerade. The attacker accesses to the system acting as an authorized user

- the attacker may have the login name and password.

Falsification. The attacker modifies or replaces valid data or produces false data

Repudiation. The attacker denies

- sending the data,
- denies receiving the data, or
- Possessing the data

Threats and Attacks

3) **Disruption**: a threat to system availability and integrity

Types of Attacks:

Incapacitation. An attack on system availability by destructing or damaging system resources (e.g., hardware) and their services.

Corruption. An attack to system integrity such that the system resources or services operate in an unintended manner.

- This can be done by a malware or an attacker that modifies system function

Obstruction. An attack to system availability by interfering, altering, or overloading communication functions

Threats and Attacks

4) **Usurpation**: a threat to system integrity

Types of Attacks:

Misappropriation. An unauthorized software uses the OS and hardware resources

- E.g., DoS attack that steals system services

Misuse. Disabling security functions, can be by the following means:

- malicious logic, or
- an attacker that gains access to the system

Threats and Assets

Four categories of assets and their attacks.

1) **Threats on hardware**: attack on system availability

   e.g., damaging or stealing the hardware

2) **Threats on software**: attack of system availability and integrity/authenticity

   e.g., deleting and damaging (availability), and modifying (integrity/authenticity) the software

3) **Threats on data**: attack on availability, integrity and confidentiality

   e.g., destroying data (availability), accessing and analyzing unauthorized data a(confidentiality), and modifying data (integrity)

Threats and Assets

4) **Threats on communication lines and networks**: can be passive or active attacks

Passive attack is performed by eavesdropping or monitoring data transmission

- The attacker only learns or makes use of information without affecting system resources
- Passive attack is hard to detect because data is not altered
  - Use attack prevention (not detection) to handle it

Two types of passive attacks.

- Release of message contents (confidentiality)
- Traffic analysis, if the data is encrypted.

Threats and Assets (cont.)

4) **Threats on communication lines and networks (cont.)**

Active attacks alters system resources or affecting their operations

- Active attack is difficult to prevent but easy to detect

Four categories of active attack:

Replay. Capture and retransmit data unit to produce an unauthorized effect

Masquerade. One entity pretends to be another entity

- It usually includes other form of attack, e.g., replay

Data modification. Alter some portion of legitimate data, delay the data, or reorder the data to produce an unauthorized effect

Denial of Service. Prevent or disallow the legitimate use of facilities

Security Functional Requirement

FIPS PUB 200 (NIST) lists 17 security related areas to protect confidentiality, integrity, and availability of systems and information stored, processed and transmitted in the system.

Countermeasures to security vulnerabilities and threats are divided into two categories:

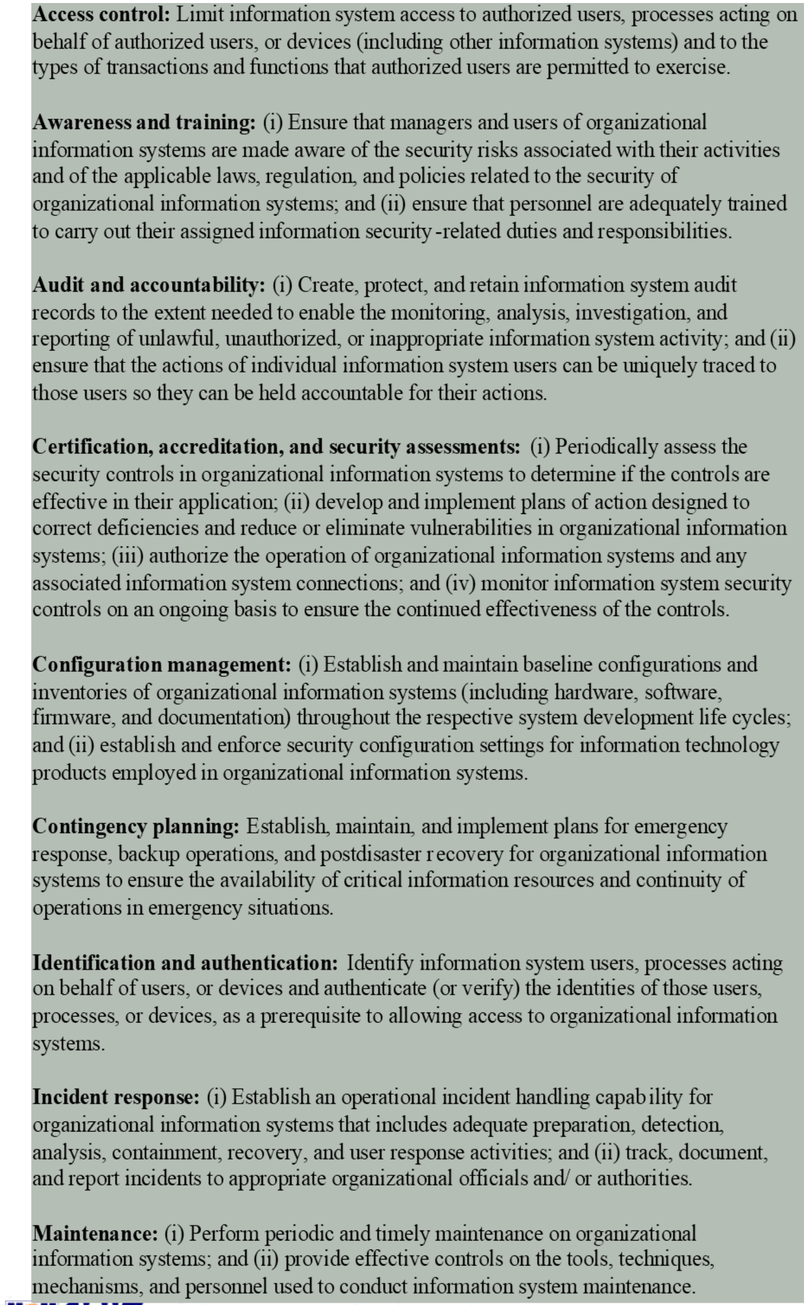
1) Those that require computer security technical measures: access control, identification and authentication, system and communication protection, system information integrity.

2) Those that are fundamentally management issues: awareness and training, audit and accountability, certification, accreditation, and security assessments, etc.

Table 1.4 (FIPS PUB 200)

Security Requirements

From Stallings & Brown textbook



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.

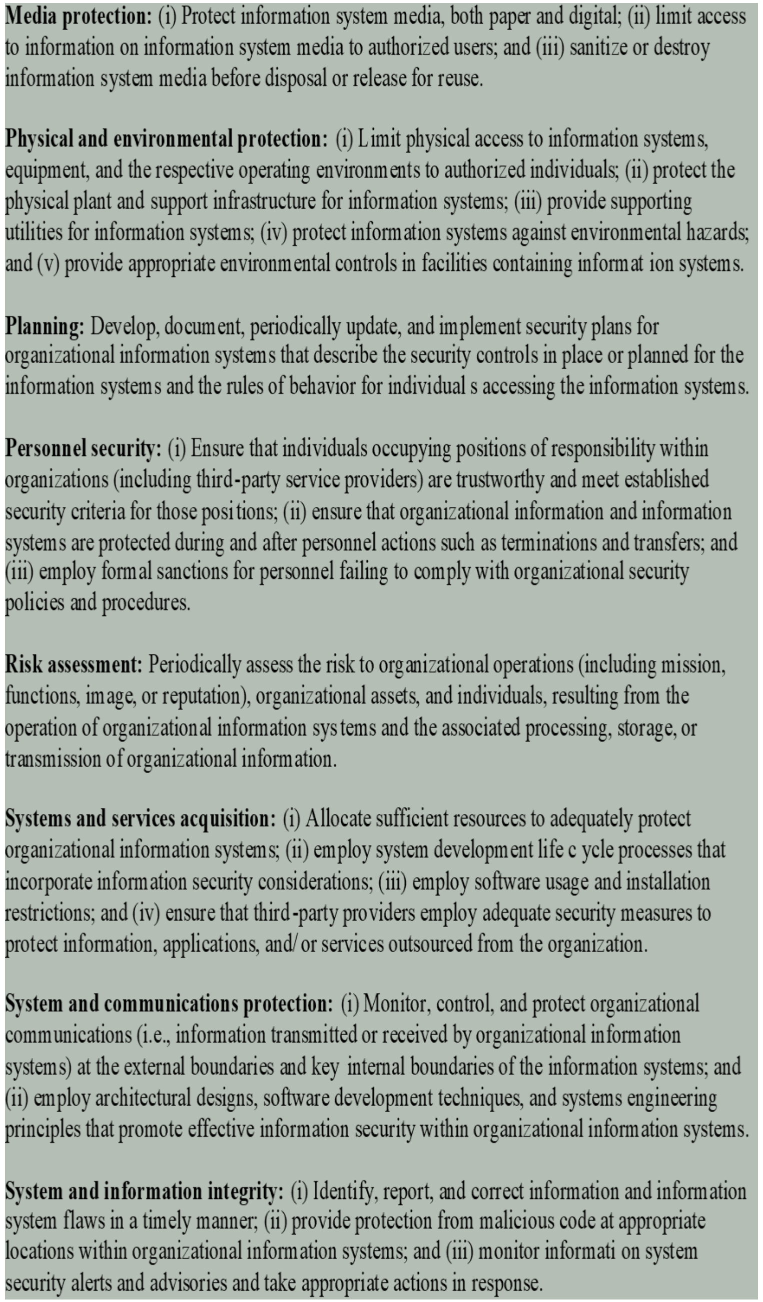
Configuration management: (i) Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration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

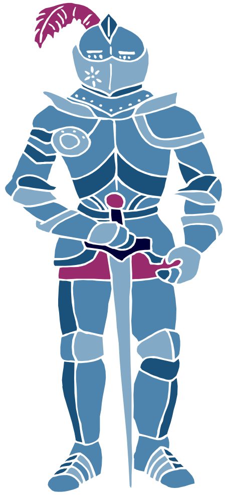
Personnel security: (i) Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected 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.



OSI Security Architecture

- The International Telecommunication Union (ITU) Recommendation X.800 defines the Security Architecture for Open System Interconnection (OSI) Architecture
  - To asses the security needs of an organization
  - To evaluate and choose various security products and policies
  - To define security requirements and approaches to satisfy the requirements

- OSI Security Architecture focuses on
  - Security Attack. Any action that compromises the security information owned by an organization.
  - Security Mechanism. A process to detect, prevent, or recover from a security attack.
  - Security Service. A service that enhances the security of the data processing systems and the information transfers of an organization to counter security attacks by making use of one or more security mechanisms

OSI Security Services

X 800 divides security services into six categories and 14 specific services.

- X800 focuses on distributed and networked systems
  - It stresses on network security than single computer security

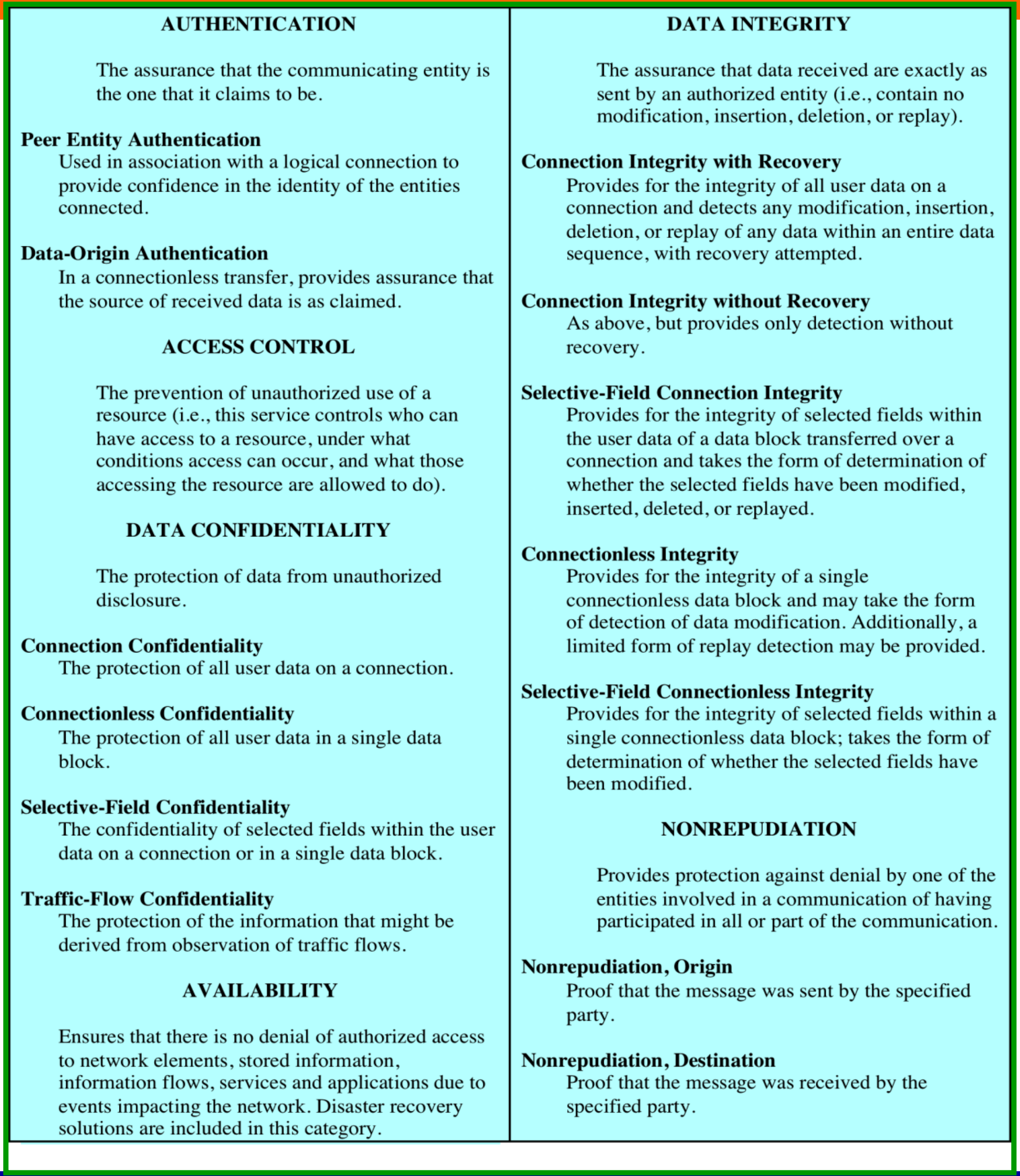
<u>Six categories of security services:</u>

1) **Authentication**. Make sure that a communication is authentic
2) **Access control**. Limit and control accesses to host systems through communication channels
3) **Data confidentiality**. Protect data from passive attacks
4) **Data Integrity**. Make sure that data received is that sent by authorized entity
5) **Nonrepudiation**. Prevent sender or receiver from denying a transmitted data.
6) **Availability**. Prevent denial of authorized access to system resources

Table 1.5

Security Services

Figure from Stallings & Brown textbook



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.

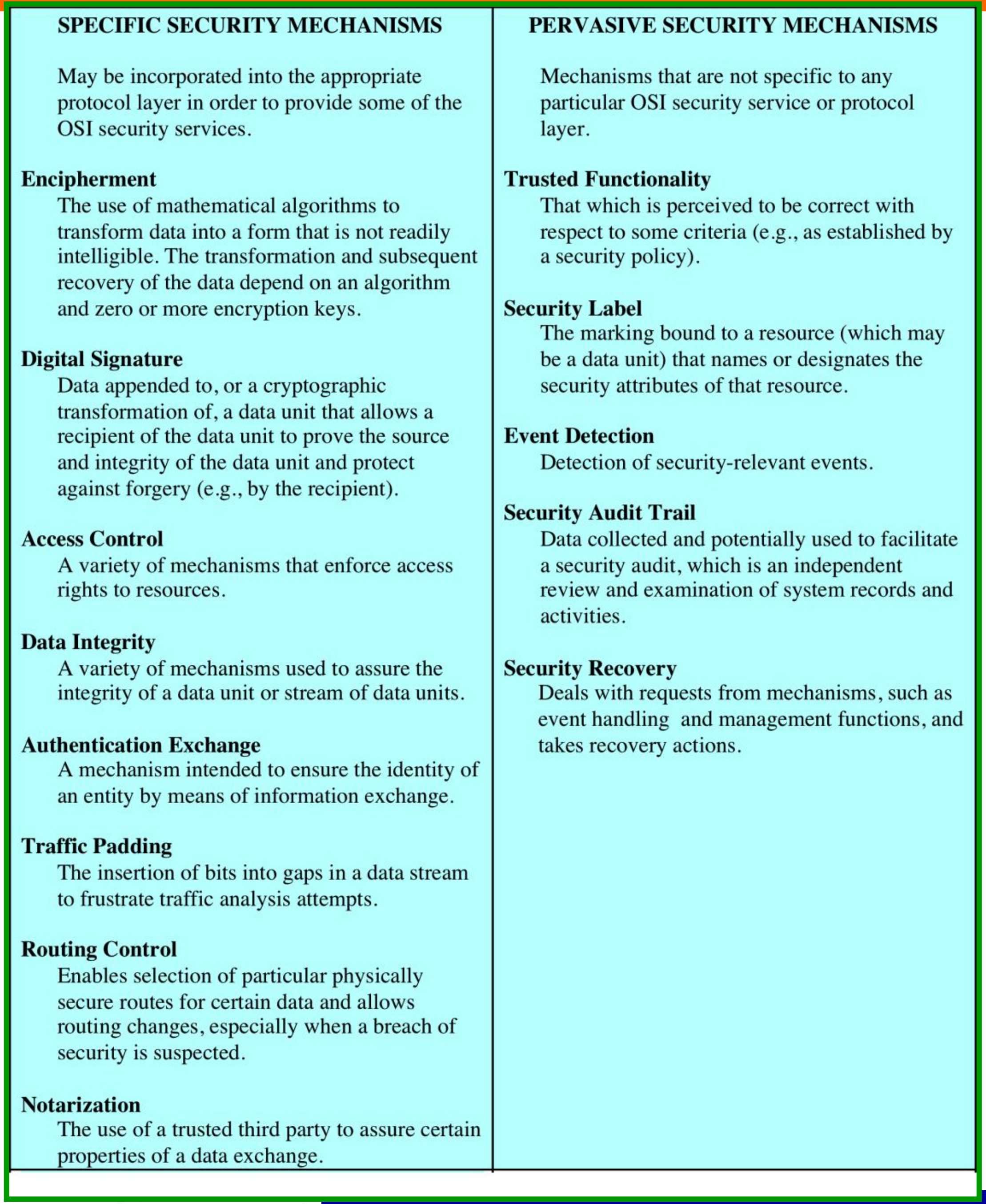
Nonrepudiation, Destination
Proof that the message was received by the specified party.

Source: From X.800, Security Architecture for OSI

OSI Security Mechanism

X800 divides security mechanism into

- Those specific to specific protocol layers and protocol applications, e.g., TCP
- Others.



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

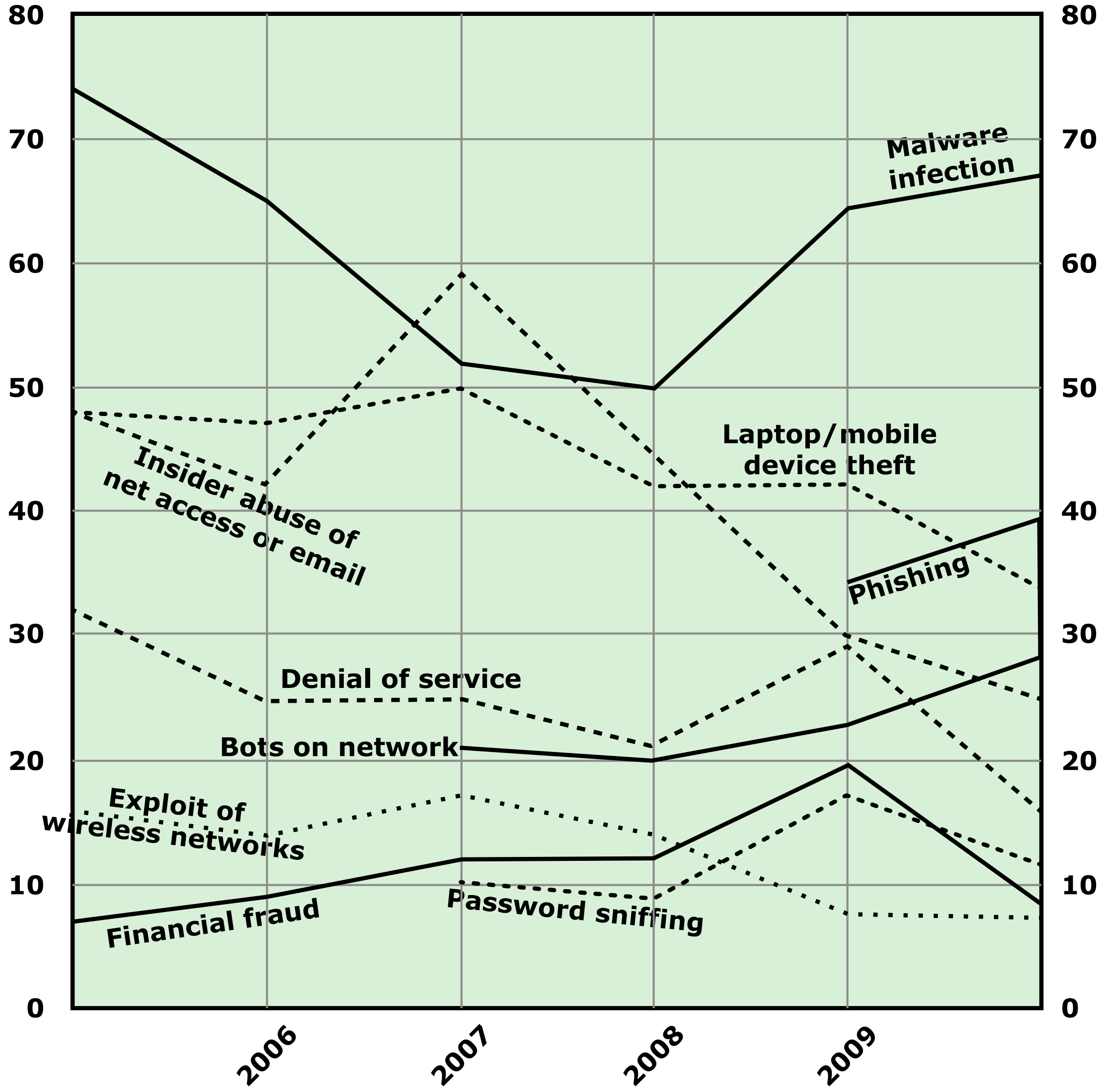
X.800 Security Mechanisms

Figure from Stallings & Brown textbook

Computer Security Trends

Survey (2010/2011) conducted by Computer Security Institute with respondents from 350 organizations in US based on

- Types of Attacks (see Fig. 1.4)
  - There is growing incidents on malware infection
- Security Technology used (See Fig. 1.5)
  - Most organizations use anti-virus software and firewalls

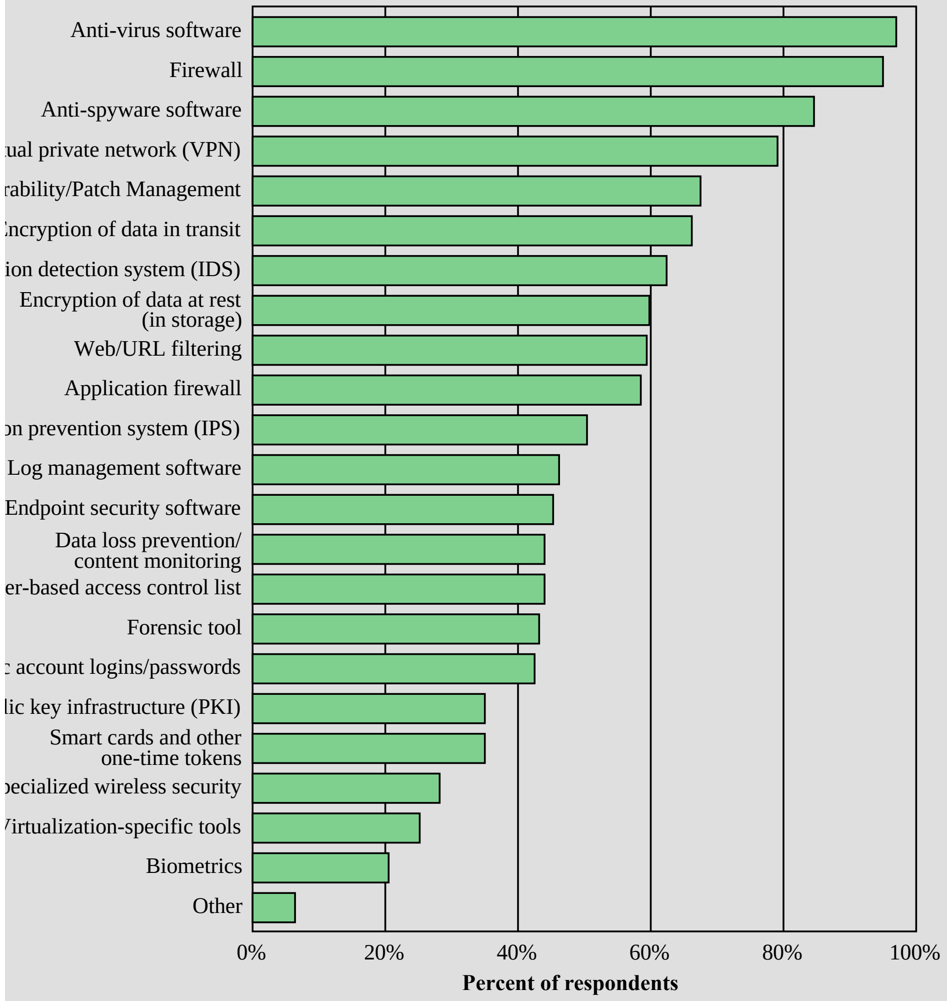


Source: Computer Security Institute 2010/2011 Computer Crime and Security Survey

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

Figure 1.4
Security Trends

Figure from Stallings
& Brown textbook



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

Figure 1.5 Security Technologies Used

Figure from Stallings & Brown textbook

Computer Security Strategy

Lampson suggests a security strategy to include three aspects

- **Specification/policy**: What to do
- **Implementation/mechanisms**: How to do it
- **Correctness/assurance**: Does it work

<u>Factors to considers for Security Policy</u>:

- The value of the assets to be protected
- The system's vulnerabilities
- Potential threats and their possible attacks
- Ease of use versus security
- Cost of security versus cost of security failure and recovery

Computer Security Strategy (cont.)

Security implementation includes these four complementary actions:

- **Prevention**
  - This is an ideal case; but not always feasible
- **Detection**
  - When prevention is not possible, detect security attacks
  - Can use intrusion detection
- **Response**
  - When an attack is detected, respond to halt the attack or prevent further damage
- **Recovery**
  - Recover from the attack by using, for example, a backup copy

Computer Security Strategy (cont.)

NIST defines **assurance** as:

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

- Does the security system design meet its requirements?
- Does the security system implementations meet its specifications?

Evaluation is the process of examining a computer product or system with respect to certain criteria

- Involves testing and analysis