

Advanced data Security

Part I: Cryptography and Network Security

Prepared by:
Dr. Hamssa Hasrouny
Info2-DataScience

Chapter 1

Overview

Standards Organizations

- **National Institute of Standards and Technology (NIST)**, U.S. federal agency
 - deals with measurement science, standards, and technology.
 - NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact.
- **Internet Society (ISOC)**, a professional membership society,
 - provides leadership in addressing issues that confront the future of the Internet
 - is organization home for groups responsible of Internet infrastructure standards published as Requests for Comments (**RFCs**).
- **International Telecommunication Union (ITU-T)**, international organization within United Nations System including government and private sector
 - mission is the development of technical standards covering all fields of telecommunications published as Recommendations.
- **International Organization for Standardization (ISO)**, a nongovernmental organization,
 - promotes the development of standardization and related activities.
 - with a view to facilitating the international exchange of goods and services
 - developing cooperation in the spheres of intellectual, scientific, technological, and economic activity.
 - ISO publishes International standards covering international agreements.

Cryptographic algorithms and protocols can be grouped into four main areas:

Symmetric encryption

- Used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords

Asymmetric encryption

- Used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures

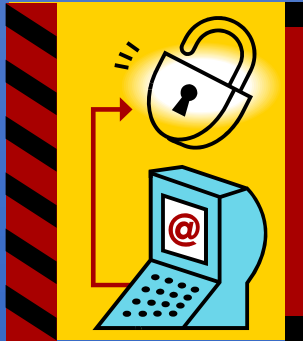
Data integrity algorithms

- Used to protect blocks of data, such as messages, from alteration

Authentication protocols

- Schemes based on the use of cryptographic algorithms designed to authenticate the identity of entities

The field of network and Internet security consists of:



measures to deter,
prevent, detect, and
correct security
violations that involve
the transmission of
information

Computer Security

- 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)

Computer Security Objectives

Confidentiality

- Data confidentiality
 - Assures that private or confidential information is not made available or 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

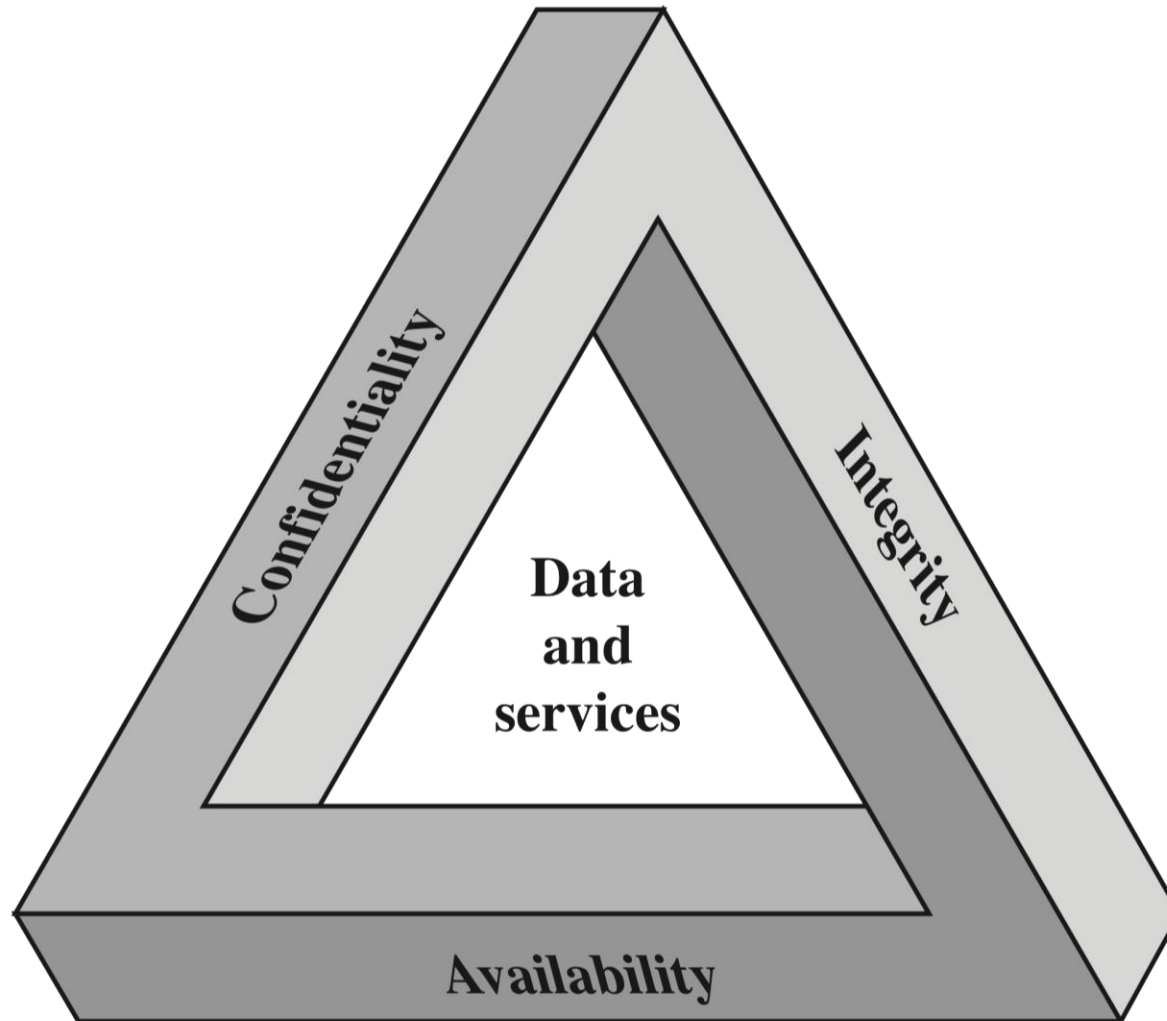
Integrity

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

Availability

- Assures that systems work promptly and service is not denied to authorized users

CIA Triad



FIPS 199 characterization of CIA:

Confidentiality

- Preserving authorized restriction on information access and disclosure, including means for protecting personal privacy and proprietary information. a loss of confidentiality is the unauthorized disclosure of information.

Integrity

- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Availability

- Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Possible additional concepts:

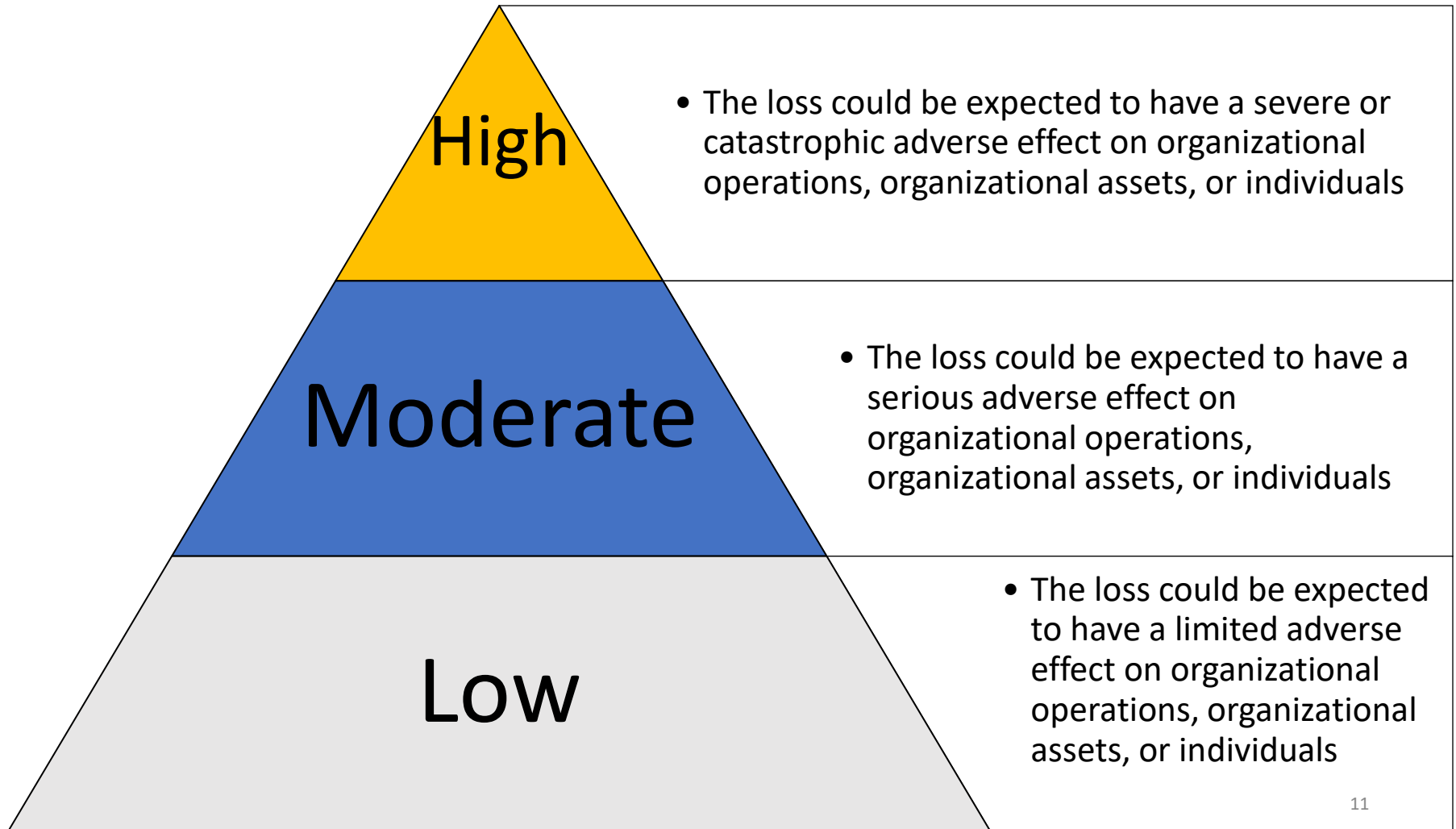
Authenticity

- Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity

Breach of Security Levels of Impact



Breach of Security

Levels of Impact examples

Low

- degradation in mission capability to an extent and duration that the organization can still perform its functions, but the effectiveness of the functions are noticeably reduced;
- minor damage to organizational assets;
- minor harm to individuals.

Moderate

- significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
- significant damage to organizational assets;
- significant financial loss;
- significant harm to individuals that does not involve loss of life or serious, life-threatening injuries.

High

- severe degradation in or loss of mission capability to an extent or duration that the organization is not able to perform its primary functions;
- major damage to organizational assets;
- major financial loss;
- severe or catastrophic harm to individuals involving loss of life or serious, life-threatening injuries.

Computer Security Challenges

- Security is not simple
- Potential attacks on the security features need to be considered
- Procedures used to provide particular services are often counter-intuitive
- It is necessary to decide where to use the various security mechanisms
- Requires constant monitoring
- Is too often an afterthought
- Security mechanisms typically involve more than a particular algorithm or protocol
- Security is essentially a battle of wits between a perpetrator and the designer
- Little benefit from security investment is perceived until a security failure occurs
- Strong security is often viewed as an impediment to efficient and user-friendly operation

OSI Security Architecture

- The OSI security architecture (X.800) is useful to managers as a way of organizing the task of providing security.
 - **Security attack**
 - Any action that compromises the security of information owned by an organization
 - **Security mechanism**
 - A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack
 - **Security service**
 - A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization
 - Intended to counter security attacks, and they make use of **one or more security mechanisms** to provide the service

Threats and Attacks (RFC 4949)



Threat

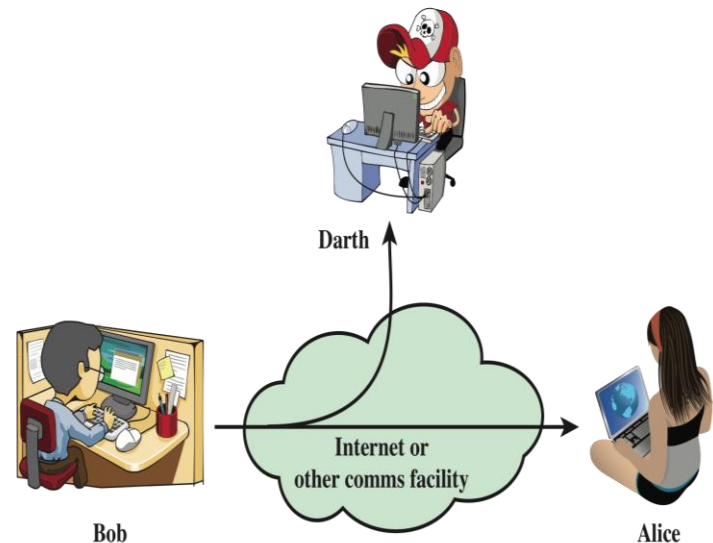
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

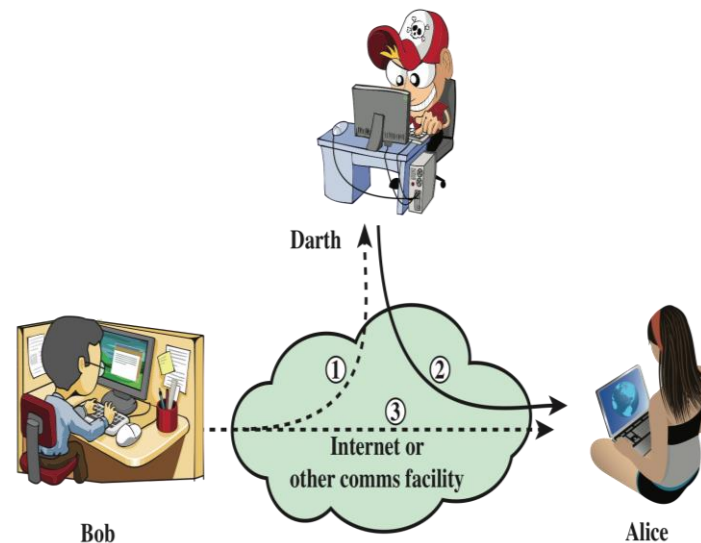
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Security Attacks

- A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of *passive attacks* and *active attacks*
- A **passive attack** attempts to learn or make use of information from the system but **does not affect system resources**
- An **active attack** attempts to alter system resources or affect their operation



(a) Passive attacks



(b) Active attacks

Figure 1.1 Security Attacks

Passive Attacks

- Are in the nature of eavesdropping on, or monitoring of, transmissions.
- Goal of the opponent is to obtain information that is being transmitted.
- Passive attacks are **very difficult to detect**. They do not involve any alteration of data.
- Two types of passive attacks are:
 - *The **release of message contents** :*
 - telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.
 - ***Traffic analysis**:*
 - even in place of encryption protection, the opponent might still be able to observe the pattern of these messages.
 - He could determine the location and identity of communication hosts and observe the frequency and length of messages being exchanged.



➤ Prevention rather than detection

Active Attacks

- Involve some modification of the data stream or the creation of a false stream
- **Difficult to prevent** because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to **detect attacks and to recover from** any disruption or delays caused by them



Masquerade

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

Modification of messages

- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

Denial of service

- Prevents or inhibits the normal use or management of communications facilities

Security Services

Security services implement security policies and are implemented by security mechanisms.

- Defined by X.800 as:
 - A service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers
- Defined by RFC 4949 as:
 - A **processing or communication service provided by a system to give a specific kind of protection to system resources**

X.800 Service Categories

X.800 divides these services into five categories

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Nonrepudiation



Authentication

- Concerned with assuring that a communication is authentic
 - In the case of a **single message**, assures the recipient that the message is from the source that it claims to be from
- In the case of ongoing interaction, assures the **two entities are authentic and that the connection is not interfered** with in such a way that a third party can masquerade as one of the two legitimate parties

Two specific authentication services are defined in X.800:

- Peer entity authentication
- Data origin authentication

Access Control

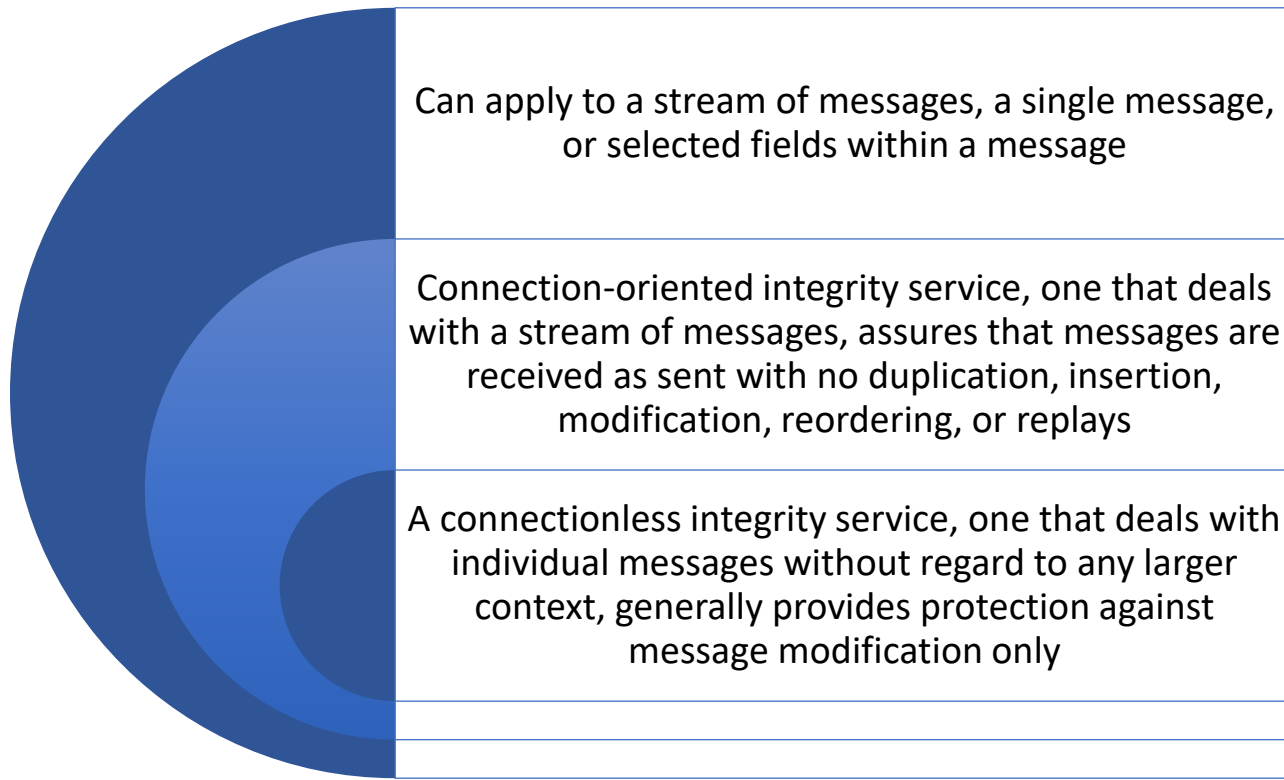
- The ability to limit and control the access to host systems and applications via communications links
- To achieve this, each entity trying to gain access must first be:
 - identified, or authenticated, so that access rights can be tailored to the individual



Data Confidentiality

- The **protection of transmitted data from passive attacks**
 - Broadest service protects all user data transmitted between two users over a period of time
 - Narrower forms of service includes the protection of a single message or even specific fields within a message
- The protection of 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

Data Integrity

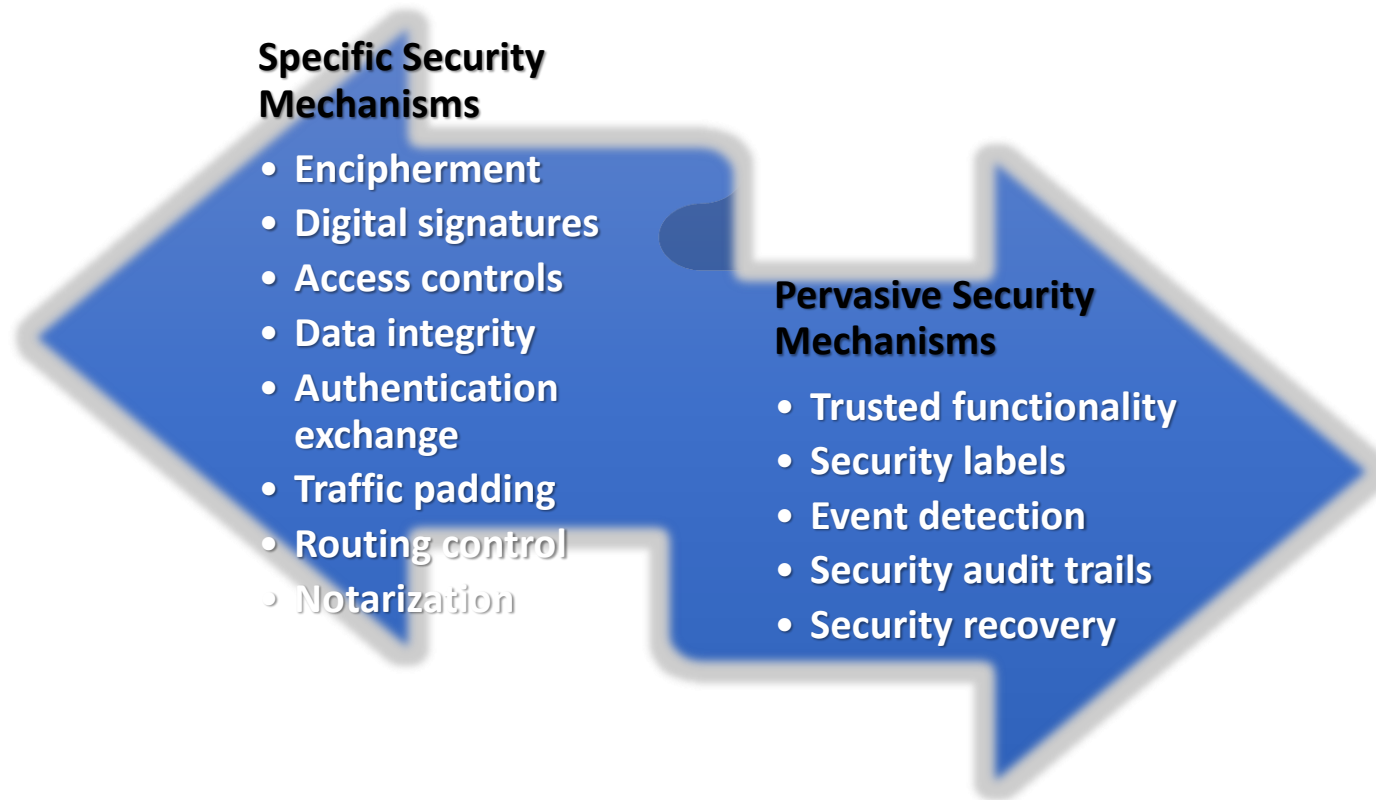


Nonrepudiation

- Prevents either sender or receiver from denying a transmitted message
- When a message is sent, the receiver can prove that the alleged sender in fact sent the message
- When a message is received, the sender can prove that the alleged receiver in fact received the message

Security Mechanisms (X.800)

X.800 divides these services into five categories and fourteen specific services



SPECIFIC SECURITY MECHANISMS

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

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.

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).

Access Control

A variety of mechanisms that enforce access rights to resources.

Data Integrity

A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Authentication Exchange

A mechanism intended to ensure the identity of an entity by means of information exchange.

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.

PERVASIVE SECURITY MECHANISMS

Mechanisms that are not specific to any particular OSI security service or protocol layer.

Trusted Functionality

That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

Security Label

The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Event Detection

Detection of security-relevant events.

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.

Security Recovery

Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Security Mechanisms (X.800)

Relationship between Security Services and Mechanism

SERVICE	MECHANISM							
	Encipherment	Digital signature	Access control	Data integrity	Authentication and exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Attack surfaces and attack trees

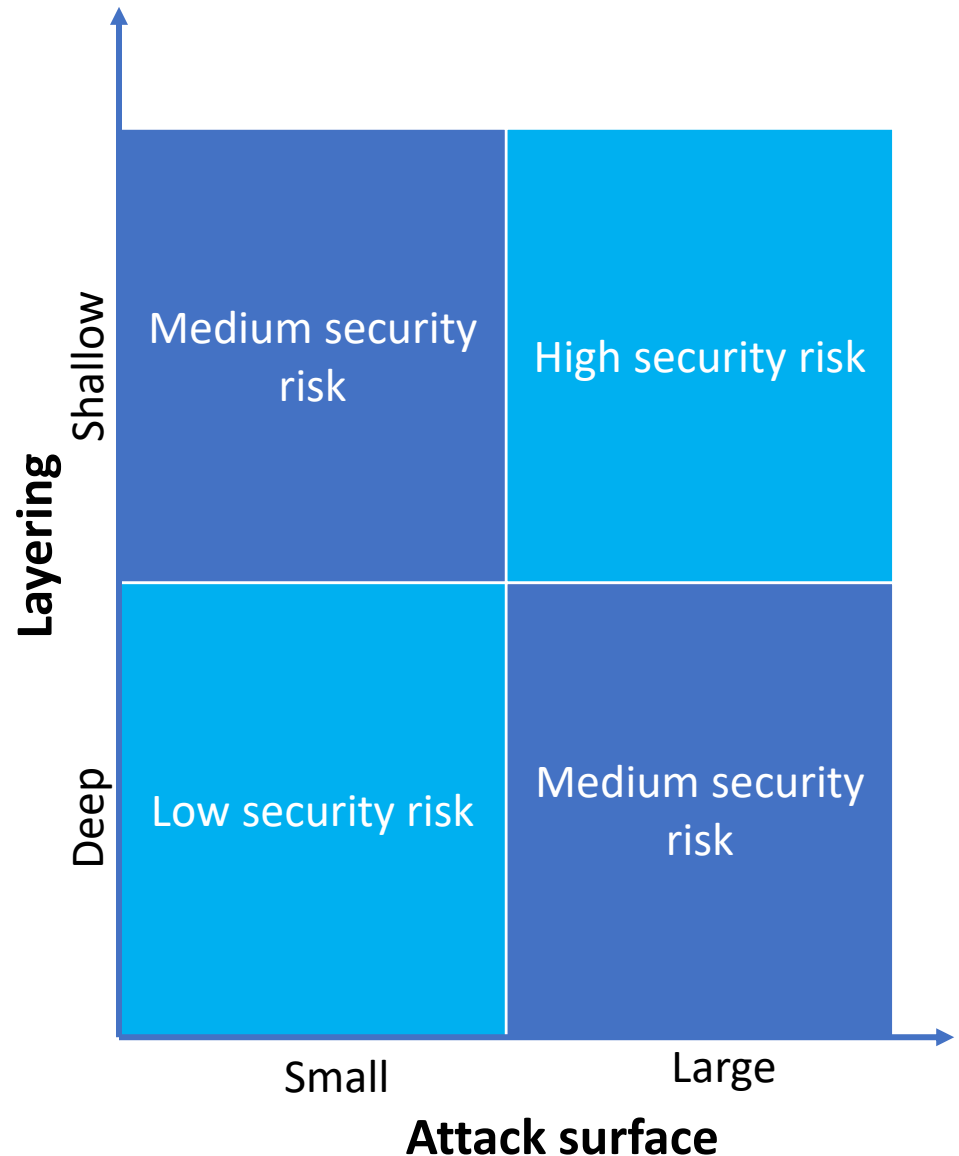
- Attack surfaces and attack trees are two concepts useful in **evaluating** and **classifying** threats.
- Attack surfaces consists of the **reachable and exploitable** vulnerabilities in a system, e.g.,
 - **Open ports** on outward facing Web and other services, and **code listening** on those ports
 - Services available on the inside of a firewall
 - Code that processes **incoming data**, email, office documents, and industry-specific custom data exchange formats
 - Interfaces, SQL, and Web forms
 - And **employee with access to sensitive information vulnerable** to a social engineering attack

Attack surfaces

- Attack surfaces can be categorized as follows:
 - **Network attack surface:** refers to vulnerabilities over an enterprise network, WAN, or the Internet e.g., DoS attack, disruption of communication links, and various forms of intruder attacks.
 - **Software attack surfaces:** refers to vulnerabilities in application, utility, or operating system code, e.g., Web server software
 - **Human surface attack:** refers to vulnerabilities created by personnel, or outsiders, such as **social engineering, human error, and trusted insiders**.
- Attack surface analysis: useful technique for assessing the scale and severity of threats to a system
 - developers and security analysts can be aware of where security mechanisms are required.

Attack surfaces

- The attack surface provides **guidance** on setting priorities for testing, **strengthening** security measures, and **modifying** the service or application.
- The use of **layering**, or defense in depth, and **attack surface reduction** complement each other in mitigating security risk.



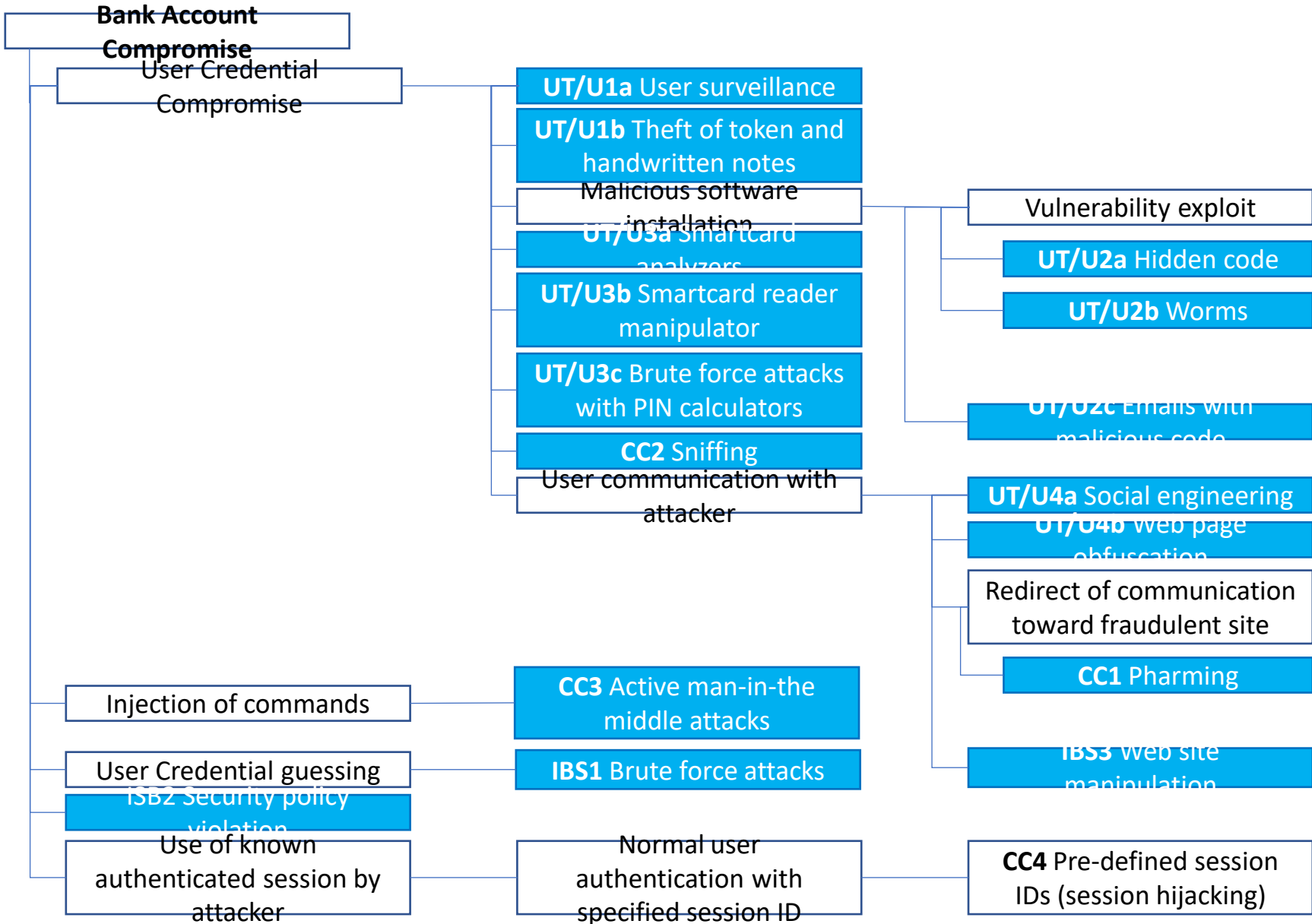
Attack Trees

- An attack tree is a **branching, hierarchical** data structure that represents a **set of potential technical techniques** for exploiting security vulnerabilities.
 - The **root node** of the tree: the security incident that is the **goal of the attack**
 - **Branches and subnodes** of the tree represent **iteratively and incrementally** the ways that an **attacker can use to reach the goal**.
 - Each subnode defines a subgoal that may have its own further subgoals, and so on.
 - The **leaf nodes** : 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.
 - To achieve the goal represented by 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.

Motivation of attack trees

- Motivation: effectively exploit the information available on attack patterns.
- CERT publish security advisories that have enabled the development of a body of knowledge about:
 - General attack strategies
 - Specific attack patterns
- **Security analyst** can use the **attack tree to document security attacks** in a structured form that **reveals key vulnerabilities**.
- The attack tree can **guide** both the **design of systems and applications, and the choice and strength of countermeasures**.

An Attack Tree study case: Internet Banking Authentication



An Attack Tree for Internet Banking Authentication : security analysis

- **Root node:** **objective** of the attacker which is to compromise a user's bank account
- **Leaf nodes:** shaded boxes which represent events that **comprise the attacks**
- All other nodes are OR-nodes.

Analysis: three components are involved in authentication:

- **User terminal and user (UT/U):** attacks targetting
 - i) the user equipment (tokens such as smartcards or other password generators),
 - ii) actions of the user;
- **Communications channel (CC):** attacks targetting the communication links
- **Internet Banking server (IBS):**
 - offline attacks against the server hosting the Internet Banking application.

An Attack Tree for Internet Banking Authentication : security analysis (con't)

- Five overall attack strategies can be identified, each of which exploits one or more of the three components:
 - User credential compromise: used against many elements of the attack surface
 - Procedural attacks
 - monitoring a user's action to observe a PIN or other credential
 - Theft of the user's token
 - Theft of handwritten notes
 - Compromise token information using token attack tools (e.g., brute-force approach or hacking the smartcard))
 - Embed malicious software to compromise user's login and password
 - Sniffing to obtain credential information via CC
 - Engage in communication with the target user
 - Injection of commands:
 - Intercept communication between the UT and the IBS to impersonate the valid user and gain access to the banking system

An Attack Tree for Internet Banking Authentication : security analysis (con't)

- User credential guessing:
 - Use random usernames and passwords to generate brute force attacks against some banking authentication
 - attack mechanism : distributed zombie PCs, hosting automated programs for username- or password- based calculation
- Security policy violation:
 - 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:
 - Attack that persuades or forces the user to connect to the IBS with a preset session ID.
 - The attacker may utilize the known session to send packets to IBS, spoofing the user's ID.

Model for Network Security

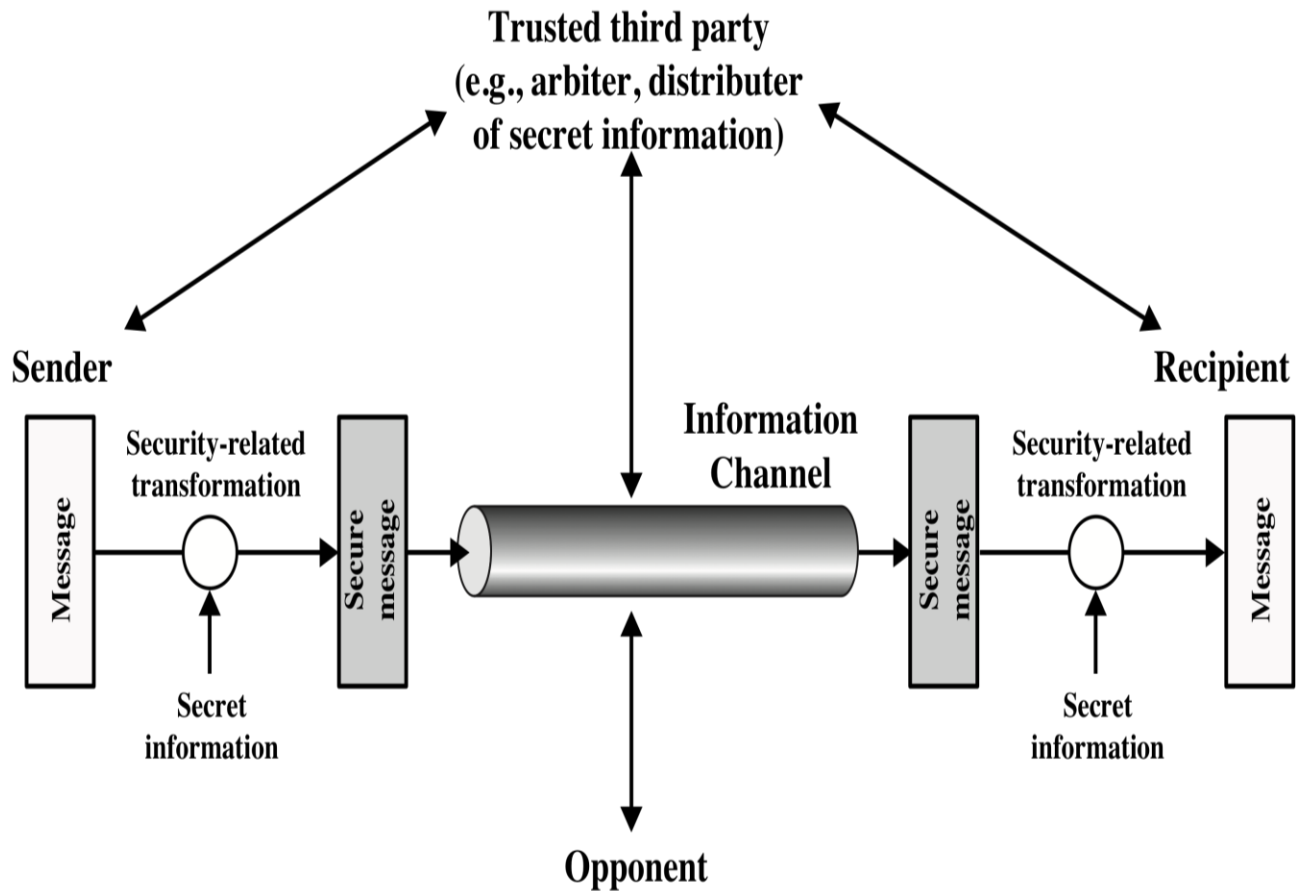


Figure 1.2 Model for Network Security

Design a particular security service

- **Four basics tasks:**

- **Design** an **algorithm** for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose;
- **Generate the secret information** to be used with the algorithm;
- Develop **methods for the distribution and sharing of the secret information**;
- Specify a **protocol** to be used by the two principals that makes of the security algorithm and the secret information to achieve a particular security service.

Network Access Security Model

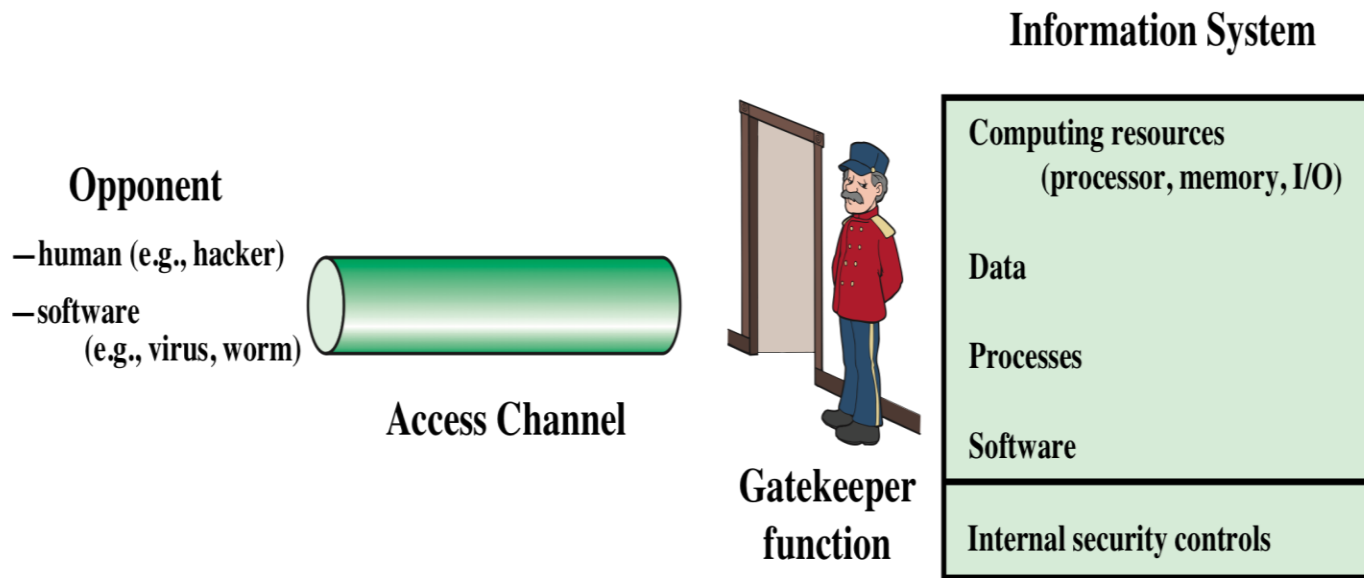


Figure 1.3 Network Access Security Model

Unwanted Access

- Placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs such as editors and compilers
- Programs can present two kinds of threats:
 - Information access threats
 - Intercept or modify data on behalf of users who should not have access to that data
 - Service threats
 - Exploit service flaws in computers to inhibit use by legitimate users
- Security mechanisms to cope with unwanted access:
 - Gatekeeper function:
 - Password-based login procedures : deny access to all but authorized users
 - Screening logic : detect and reject worms, viruses, etc.
 - Internal controls (2nd line of defense) in case an unwanted user or Software gain access:
 - Monitor activity and analyze stored information (IDS/IPS, SIEM, etc.)



Summary

- Computer security concepts
 - Definition
 - Examples
 - Challenges
- The OSI security architecture
- Security attacks
 - Passive attacks
 - Active attacks
- Security services
 - Authentication
 - Access control
 - Data confidentiality
 - Data integrity
 - Nonrepudiation
 - Availability service
- Security mechanisms