Chapter 1

INFORMATION SYSTEMS SECURITY

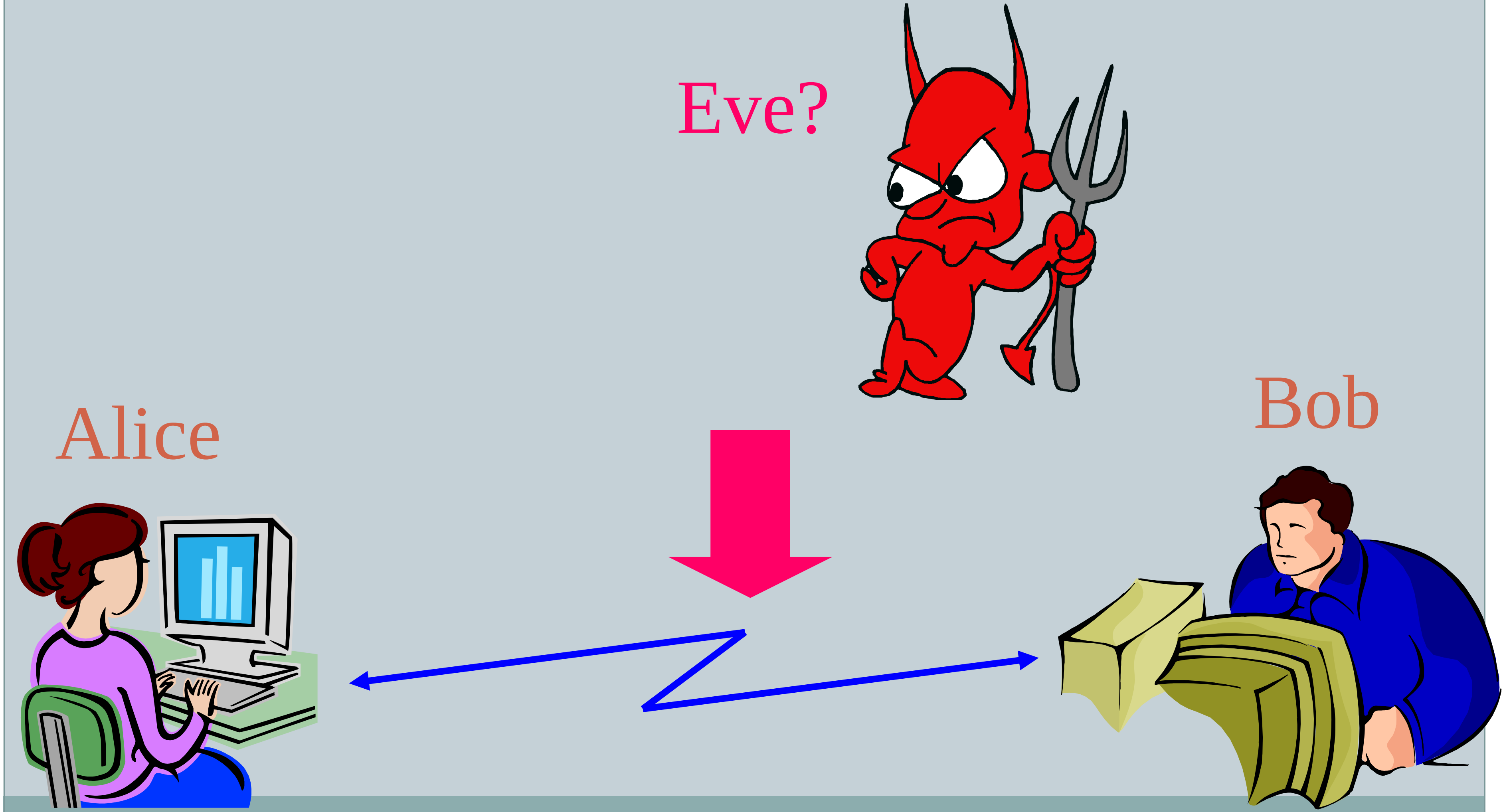
INTRODUCTION

Learning Objectives

After studying this chapter, you should be able to:

- Describe the key security requirements of confidentiality, integrity, and availability.
- Discuss the types of security threats and attacks that must be dealt with and give examples of the types of threats and attacks that apply to different categories of computer and network assets.
- Summarize the functional requirements for computer security.
- Explain the fundamental security design principles.

The Main Players

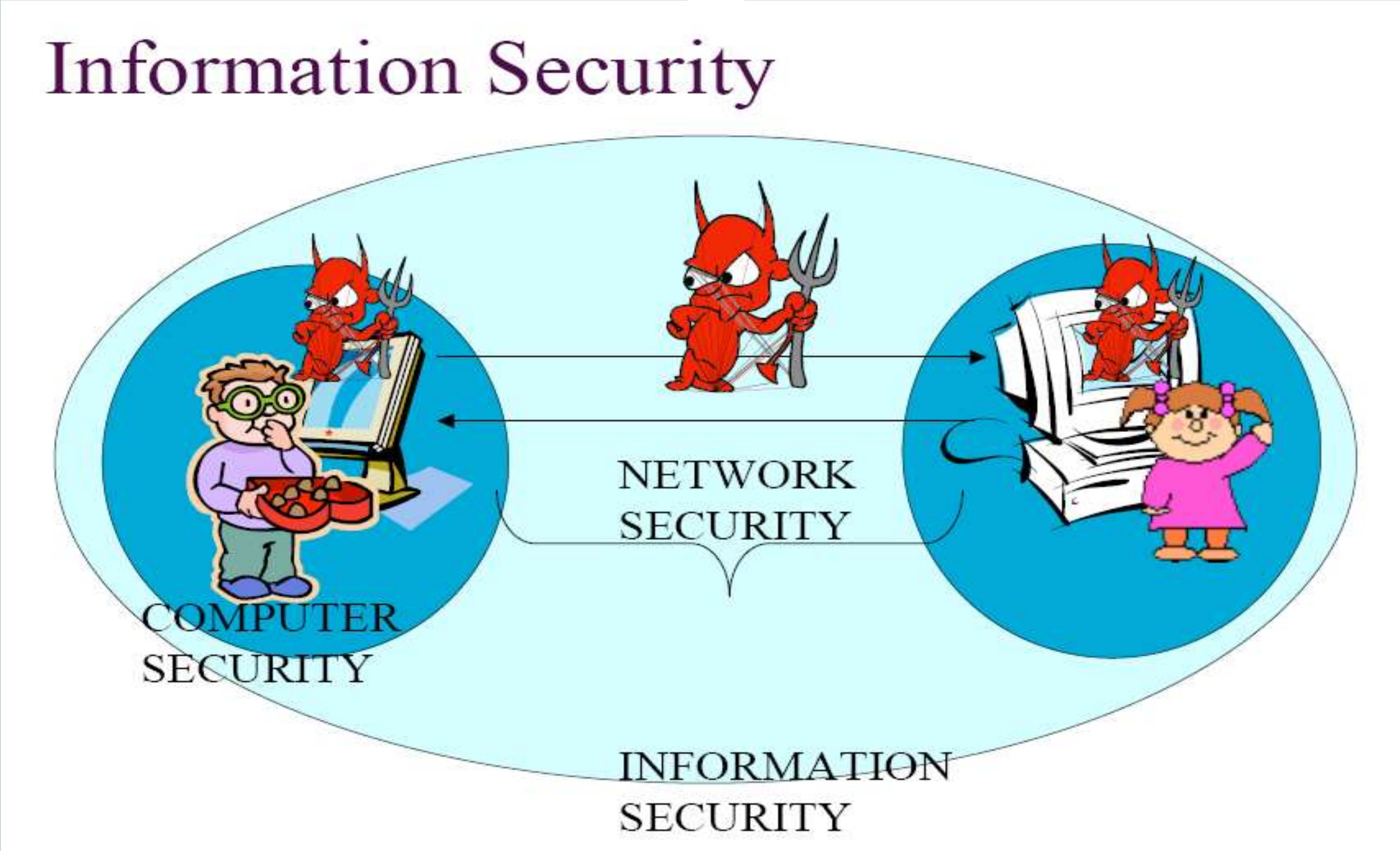


Eve?

Alice

Bob

Definitions



Information Security

Definitions

- Computer security deals with computer-related assets that are subject to a variety of threats and for which various measures are taken to protect those assets.
- Three fundamental questions:
  - 1. What assets do we need to protect?
  - 2. How are those assets threatened (vulnerable)?
  - 3. What can we do to counter those threats?
- Definition of **Computer Security (***The NIST Computer Security Handbook [NIST95]* **)**: The protection afforded to an automated information system in order to attain the applicable objectives of preserving (protecting) the integrity, availability, and confidentiality of information system resources (includes hardware, software, information/data, and telecommunications).

Definitions

- **Network Security -** measures to **protect** data **during** their **transmission**. Network security is term that describes that the policies and procedures implemented by a network administrator to avoid and keep track of unauthorized access, exploitation, modification, or denial of the network and network resources.
- **Internet Security -** measures to **protect** data **during** their **transmission** over a collection of interconnected networks.
- Internet security is a branch of computer security that deals specifically with Internet-based threats. These include hacking, where unauthorized users gain access to computer systems, email accounts or websites; viruses and other malicious software (malware), which can damage data or make systems vulnerable to other threats.
- The field of **network** and **Internet** **security** consists of measures to **deter**, **prevent**, **detect**, and **correct** security **violations** that involve the transmission of information. That is a broad statement that covers a host of possibilities.

Another Definition

- Information security can be thought of as the protection of the information system and its resources against accidental or intentional disclosure of confidential data, unlawful modification of data or programs, the destruction of data, software or hardware, and ensuring non-repudiation.
- Information systems security- refers to the processes and methodologies involved with keeping information confidential, available, and assuring its integrity.

Always Remember

- Nothing is ever completely or truly secure. There is always a way around or through any security precaution that we construct.

Realize that you are target

- Do not make the mistake of assuming that your company is too small for hackers to bother with
- Hackers are very familiar with this way of thinking.
- Hackers know "small" usually equal weak and easily exploitable!

OSI Security Architecture
Services, Mechanisms, Attacks

- We consider three aspects of information security:
  - **Security attack:** Any action that compromises the security of information owned by an organization. Or an assault (attack) on system security that develops from an intelligent threat; a planned attempt to evade (escape, avoid) security services and violate security policy of a system.
    - information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
    - a wide range of attacks
    - can focus of generic types of attacks : Passive, active
  - **Security mechanism:** A process (or a device incorporating such a process) that is designed to prevent, detect, or recover from a security attack.
    - no single mechanism can support all functions required
    - however one particular element underlies many of the security mechanisms in use: cryptographic techniques

OSI Security Architecture
Services, Mechanisms, Attacks

- **Security Service is a service that enhances the security of the data processing systems and the information transfers of an organization**
  - intended to counter security attacks
  - make use of one or more security mechanisms to provide the service
  - replicate functions normally associated with physical documents
    - Examples; have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Examples

- Identify: (a) the policies, and (b) the mechanisms that support the following:
  - Only students in an Information Security class will be given accounts on the departments computer system.

    Answer.
    - The policy is that only students in that class may use the CS Department's system.
    - The mechanism is the procedure of not giving other students an account.
  - The login program will disallow logins of any students who enter their passwords incorrectly three times.
    - Answer.
    - The policy is that only authorized students may login (so guessing is not allowed).
    - The mechanism is that after three failed attempts the system disables the account.

Examples

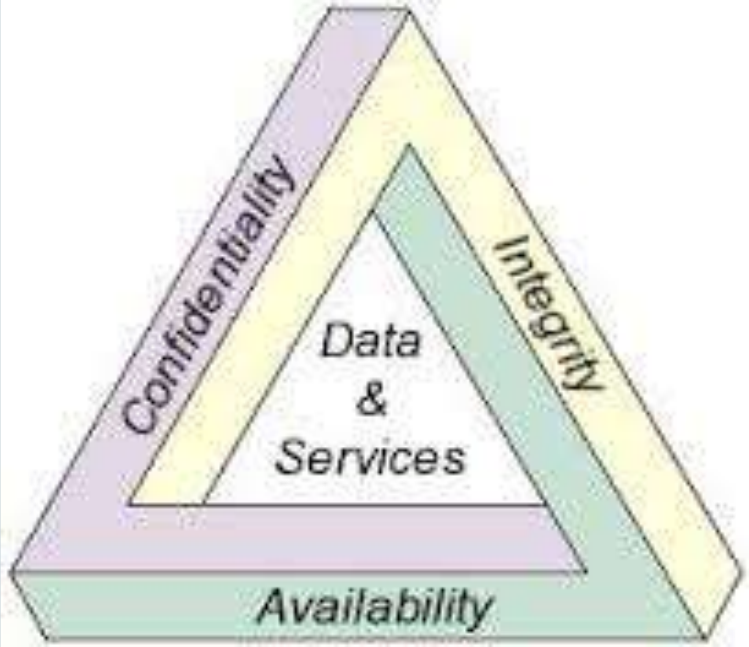
- A program used to submit homework will turn itself off just after the due date.

  Answer.

  - The policy is that late homework is not accepted.
  - The mechanism is the program disabling itself after the due date.

The Main Pillars of Security

- These three concepts form what is often referred to as the **CIA triad**.
- The three concepts represent the fundamental security objectives for both data and for information and computing services.



Computer Security Objectives

- The **definition** of **computer security** introduces three key objectives that are at the heart of computer security:
  - **Confidentiality:** ensures that computer-related assets are accessed only by authorized parties. That is, only those who should have access to something will actually get that access. By "access," we mean not only reading but also viewing, printing, or simply knowing that a particular asset exists. Confidentiality is sometimes called **secrecy** or **privacy**. So, this term covers two related concepts:
    - ✓ **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.

Computer Security Objectives

- **Integrity:** means that assets can be modified only by authorized parties or only in authorized ways. In this context, modification includes writing, changing, changing status, deleting, and creating. So, 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 intended function in an unimpaired (perfect) manner, free from deliberate or unintended unauthorized manipulation of the system.
- **Availability:** means that assets are accessible to authorized parties at appropriate times. In other words, assures that systems work promptly (on time) and service is not denied to authorized users.
  - For example: if some person or system has legitimate access to a particular set of objects, that access should not be prevented.
  - For this reason, availability is sometimes known by its opposite, denial of service.

The Main Pillars of Security

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information..
  - **Example:** Alice sends a message to Bob, only Alice and Bob can understand the content of the message.
- Integrity: Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information. (detect if data was modified, from the source to the destination)
  - **Example:** Alice sends an email to Bob. Carl intercepts the message and modifies it. Data integrity allows for Bob to detect that the message was modified on the way from Alice to him.
- 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.
  - **Example**: A web site might become unavailable if the server crashes, or is bombarded with requests.

Possible additional concepts:

- Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. AAA (A triple A Security)
  - **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. **This means 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. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after action recovery and legal action.**

Possible additional concepts:

- **The most commonly mentioned are as follows:**
  - **Authentication** is any process by which you verify that someone is who they claim they are. This usually involves a username and a password, but can include any other method of demonstrating identity, such as a smart card, retina scan, voice recognition, or fingerprints. (is the process of verifying an identity previously established in a computer system – Password and other authentication factors)
    - ✓ Data source authentication: the data is coming from an authorized party.
      - ✓ Example: Alice receives a message from Bob. This service ensures that the message is from Bob and not from (Eve) Carl.
    - ✓ Entity authentication: the entity is who it says it is.
      - ✓ Example: When Alice tries to obtain access to her bank account, an authentication operation is performed to ensure that Alice asks for the information.

Key Security Concepts

- **The most commonly mentioned are as follows:**
  - **Non-repudiation:** means that the sender or generator of information cannot deny that he did send or generate the information.
  - The goal of Non-repudiation is to provide protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. So, neither the sender, nor the receiver of a message are able to deny the transmission.
  - Nonrepudiation, Origin: Proof that the message was sent by the specified party.
  - Nonrepudiation, Destination: Proof that the message was received by the specified party.
    - ✓ Example: Alice sends Bob a contract, signed. The nonrepudiation service ensures that Alice can not claim that the signature was produced by somebody else.
  - **Access control:** only authorized parties can use specific resources. **(The process of permitting or denying access to a specific resource – What access do you have?)**
    - ✓ Example: Alice wants to print a document, she must be authorized to get that document and to use the printer.

Key Security Concepts

- There are three levels of impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability).
  - **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 for Security Services

- **Confidentiality**
  - Student grade information is an asset whose confidentiality is considered to be highly important by students. Grade information should only be available to students, their parents, and employees that require the information to do their job.
  - Student enrollment information may have a moderate confidentiality rating.
  - Directory information, such as lists of students or faculty or departmental lists, may be assigned a low confidentiality rating or indeed no rating. This information is typically freely available to the public and published on a University Web site.

Examples for Security Services

- **Integrity**
  - Hospital patient's allergy information stored in a database. The doctor should be able to trust that the information is correct and current. Now suppose that an employee (e.g., a nurse) who is authorized to view and update this information. Patient allergy information is an example of an asset with a high requirement for integrity.
  - An example of an asset that may be assigned a moderate level of integrity requirement is a Web site that offers a forum to registered users to discuss some specific topic. Either a registered user or a hacker could falsify some entries or deface the Web site.

Vulnerabilities, (Threats ,Attacks), and Countermeasures

- Vulnerabilities
  - A weakness in the security system implementation or operation (Moreover vulnerabilities are considered to be hidden doors or loopholes within the applications and network or other)
  - Can make assets is corrupted, leaky, unavailable.
  - E.g. a program flaw, poor security configuration, bad password policy
- Threat
  - A set of situations (circumstances) or people that potentially causes loss or harm to a system (Potential violation of security policy by exploiting a vulnerability)

Vulnerabilities, (Threats ,Attacks), and Countermeasures

- Attack
  - An action or series of actions to harm a system
  - A threat that is carried out, successful attack lead to violation of security policy.
  - Active attack: attempt to alter system resources or operation.
  - Passive attack: attempt to learn information that does not affect system resources.
  - Inside attack: initiated by entity with authorized access to system.
  - Outside attack: initiated by unauthorized user of system.

Vulnerabilities

- Security polices and products may reduce the likelihood that an attack will actually be able to penetrate your system's defenses, or they may require an intruder to invest so much time and so many resources that it's just not worth it - but there's no such thing as a completely secure system.

- Typical points of vulnerability in a computer systems.
- Physical vulnerabilities:
  - Your building and computer rooms are vulnerable. Intruders can break into your computer facilities just as they break into your home.
  - Once in they can sabotage and vandalize your computer, and they can steal diskettes, disk packs, tape reels and printout.
- Natural vulnerabilities:
  - Natural disasters and to environmental threats. such as: fire, flood, earthquakes, lightning, and power loss can wreck your computer and destroy your data. Dust, humidity, and uneven temperature conditions can also do damage.

- Hardware and software vulnerabilities:
  - Certain kind of hardware failures. (e.g. many systems provide into hardware protection by structuring memory privileged and nonprivileged areas.
  - Software: bugs in security features may open the floodgates to accidents or intrusion.
- Media vulnerabilities:
  - disk packs, tape reels and printout can be stolen or can be damaged.
- Emanation vulnerabilities:
  - All electronic equipment emits electrical and electromagnetic radiation. Electronic eavesdroppers can intercept the signals emanating from computer systems and networks, and can then decipher them.

- Communication vulnerabilities:
  - if your computer is attached to a network, or even if it can be accessed by telephone, your greatly increase the risk that someone will be able to penetrate your system. messages can be intercepted, misrouted, and forged.
- Human vulnerabilities:

Countermeasures

- A **countermeasure** is any means (ways) taken to deal with a security attack. Ideally, a countermeasure can be devise (set up , developed, planned) to **prevent** a particular type of attack from succeeding. When prevention is not possible, or fails in some instance, the goal is to **detect** the attack, and then **recover** from the effects of the attack.
- means used to deal with security attacks
  - ✓ **prevent**
  - ✓ **detect**
  - ✓ **recover**

Computer Security Terminology

- **Adversary (threat agent):** An entity that attacks, or is a threat to, a system.
- **Attack:** An assault (violate) on system security that comes from an intelligent threat; that is, an intelligent 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 (probability, chance) 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.

Computer Security Terminology

- **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 (possible) 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.

Security Concepts and Relationships

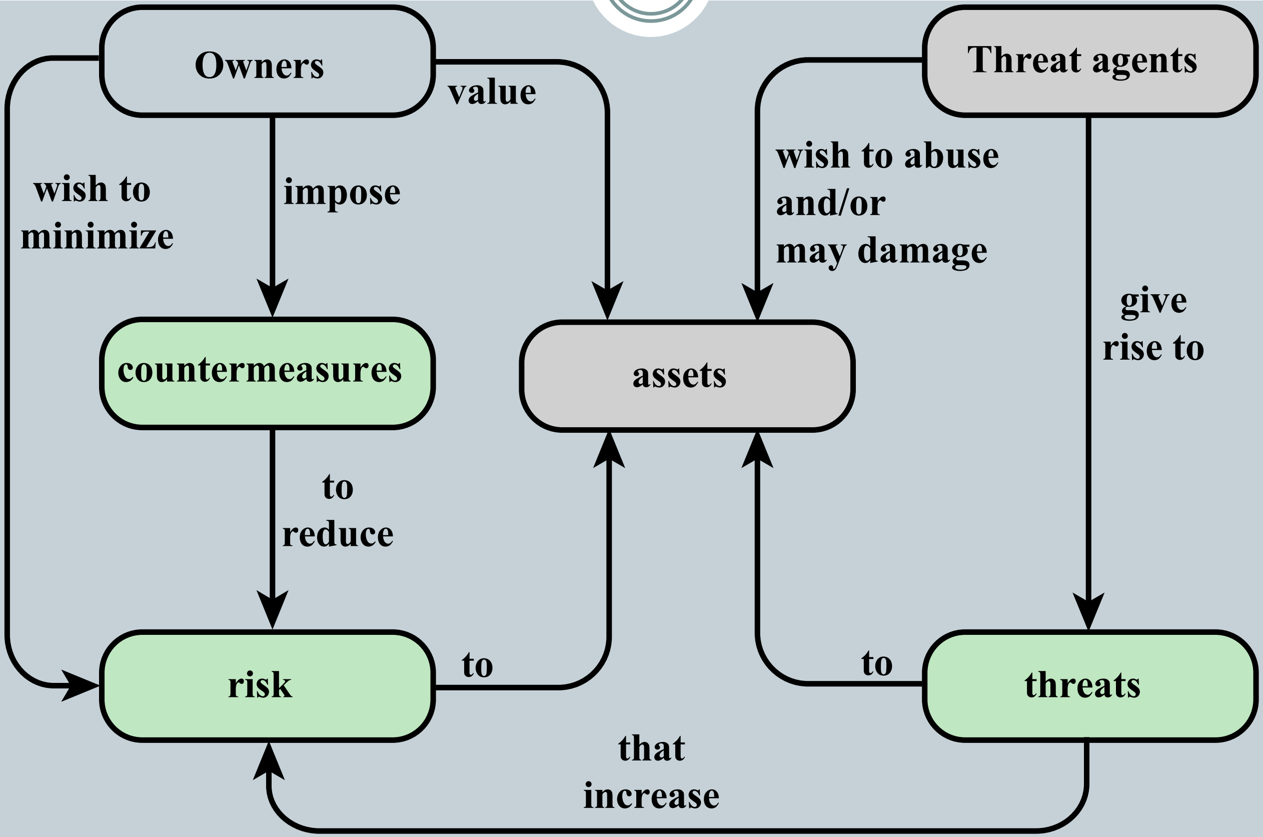
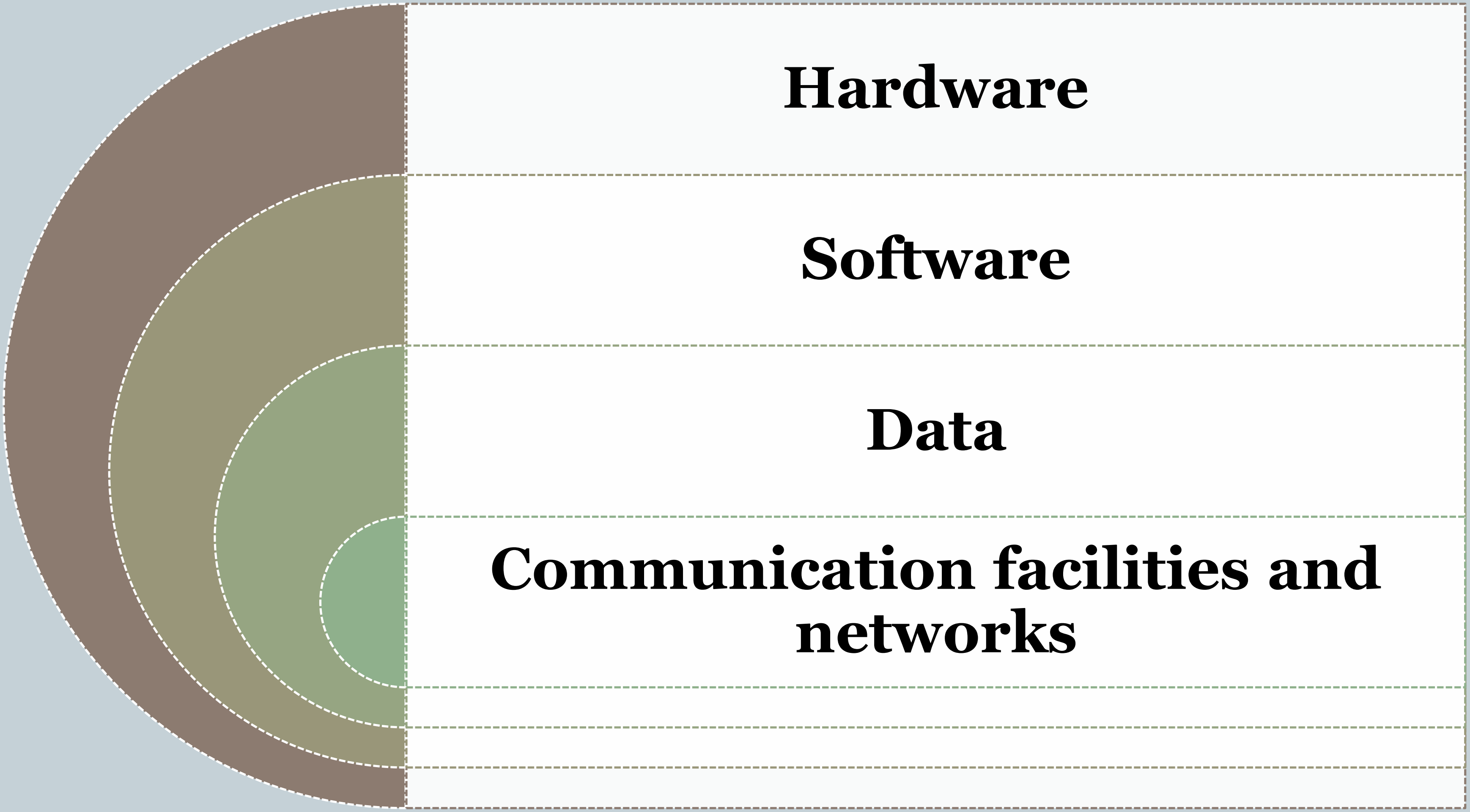


Figure 1.1 Security Concepts and Relationships

Assets of a Computer System



Hardware

Software

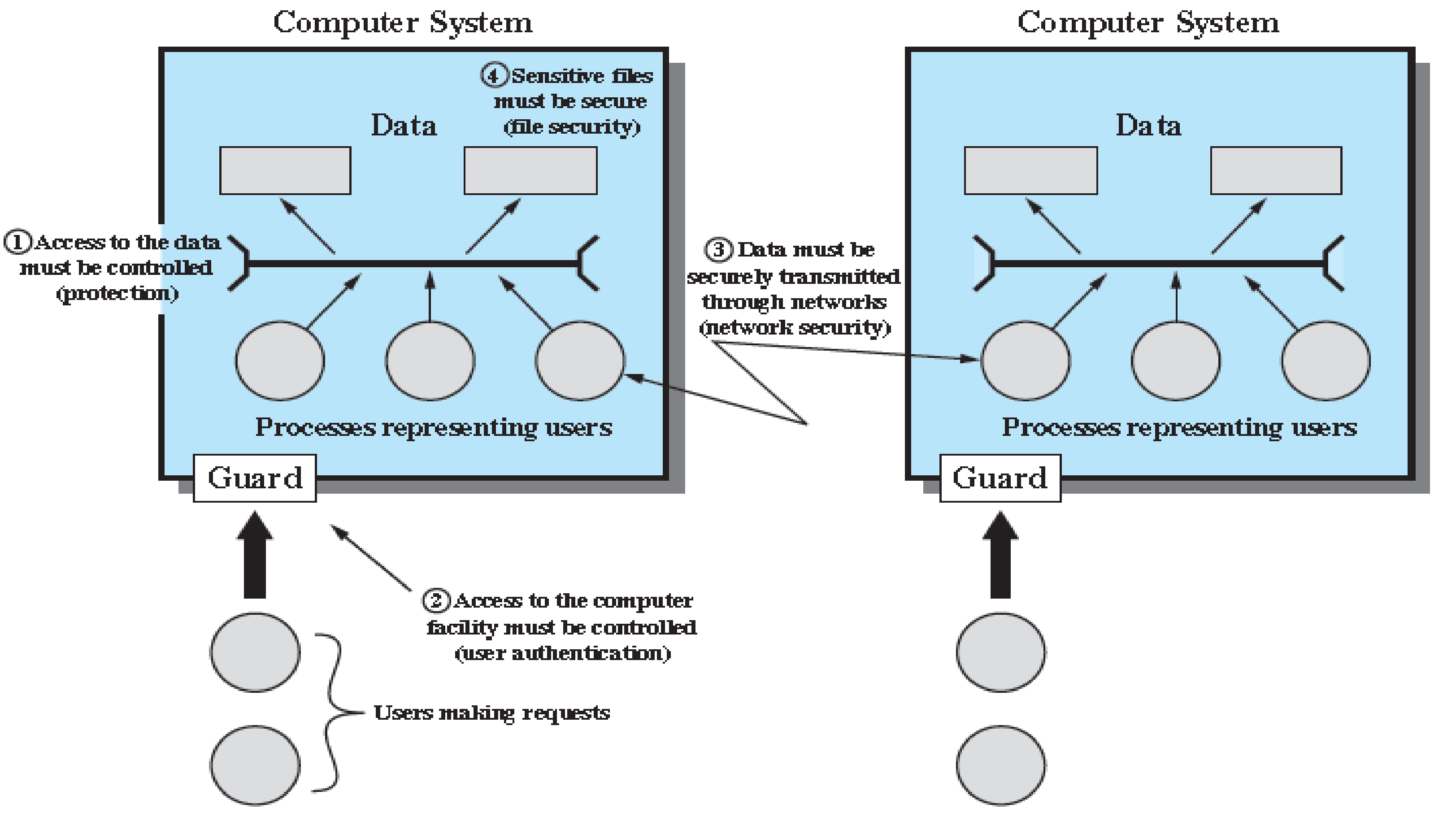
Data

Communication facilities and networks

Assets of a Computer System

- The assets of a computer system can be categorized as follows:
  - 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.

Scope of Computer Security.



Computer System
Data
4 Sensitive files must be secure (file security)
1 Access to the data must be controlled (protection)
Processes representing users
Guard
2 Access to the computer facility must be controlled (user authentication)
Users making requests
3 Data must be securely transmitted through networks (network security)
Computer System
Data
Processes representing users
Guard

Figure 1.2 Scope of Computer Security

Note: This figure depicts security concerns other than physical security, including controlling of access to computers systems, safeguarding of data transmitted over communications systems, and safeguarding of stored data.

Computer and Network Assets, with Examples of Threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Network Security Attacks

- Network security attacks can be classified as:
  - 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.
- Passive attacks are in the nature of eavesdropping on, or monitoring of transmissions. The goal of the attacker is to obtain information that is being transmitted.

Network Security Attacks

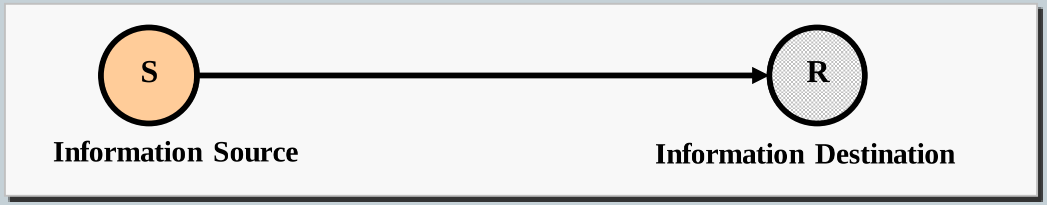
- Passive Attacks
  - The goal is to obtain information that is being transmitted.
  - E.g. Release of confidential information and Traffic analysis
  - Difficult to detect -> not alter data -> nobody realizes the existence of the third party
  - Initiative to launch an active attack
  - Interception
  - May be relieved by using encryption

Types of Attacks

- To devise controls, we must know as much about threats as possible. We can view any threat as being one of four kinds:
- Interception
  - Attack on Confidentiality
- Interruption
  - Attack on Availability
- Modification
  - Attack on Integrity
- Fabrication
  - Attack on Authenticity

Network Security Attacks

- **The attacker is an entity trying to disturb the normal flow of transmission data in a network system.**

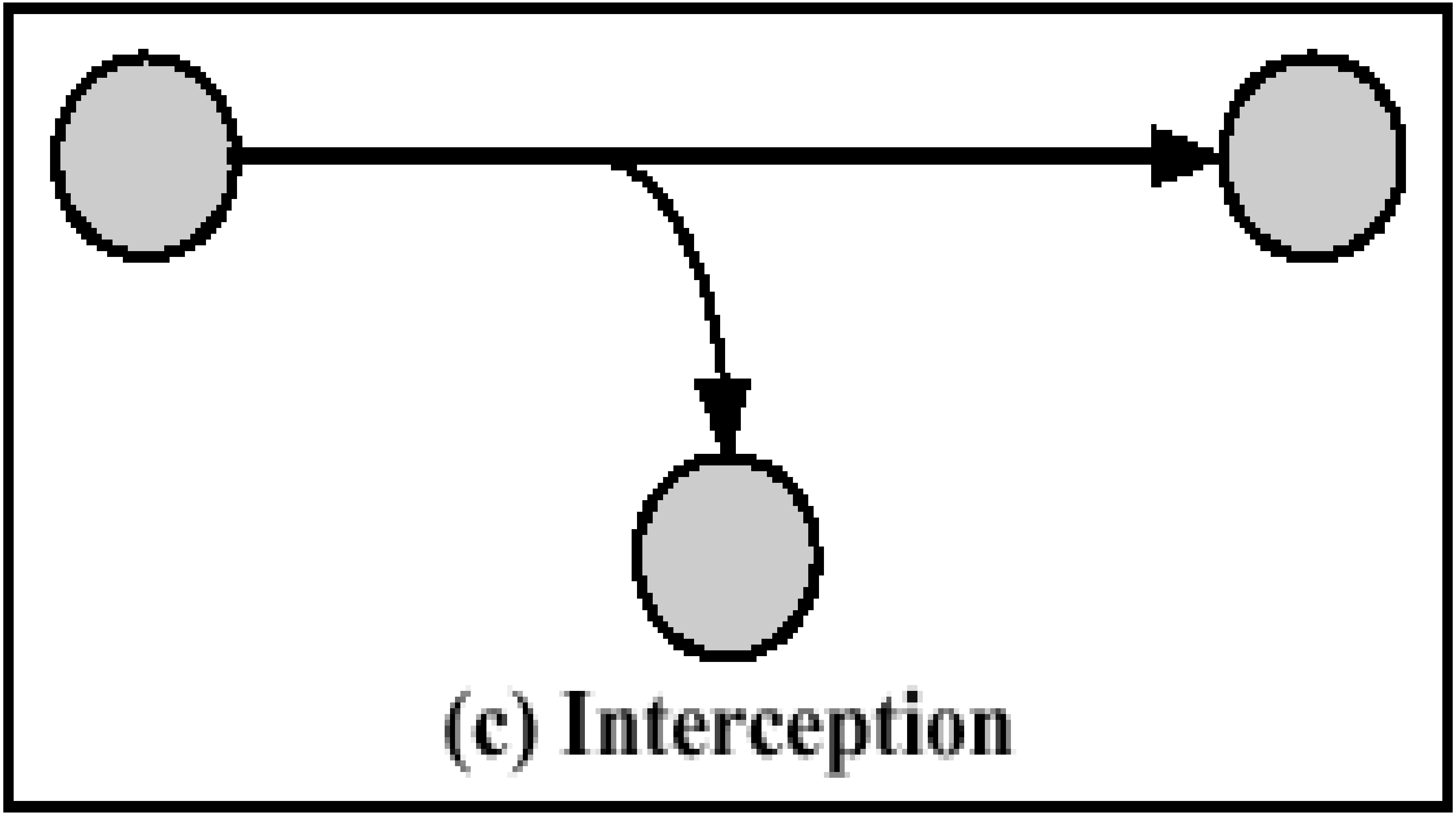


Normal data flow

Interception (Eavesdropping)

- Information disclosure/information leakage. An unauthorized party gains access to an asset.
- This is an attack on confidentiality like tapping a conversation between parties. Difficult to trace as no traces of intrusion might be left.
- The unauthorized party could be a person, a program, or a computer.
- Examples include:
  - wiretapping (eavesdropping, sniffing) to capture data in a network, the illicit (illegal) copying of files or programs
- This attack is a passive attack . Here the attacker could be eavesdropping on network traffic between the transmitter and receiver to capture data in a network without altering the information itself.
- The countermeasure against this attack is encryption.

Interception (Eavesdropping)

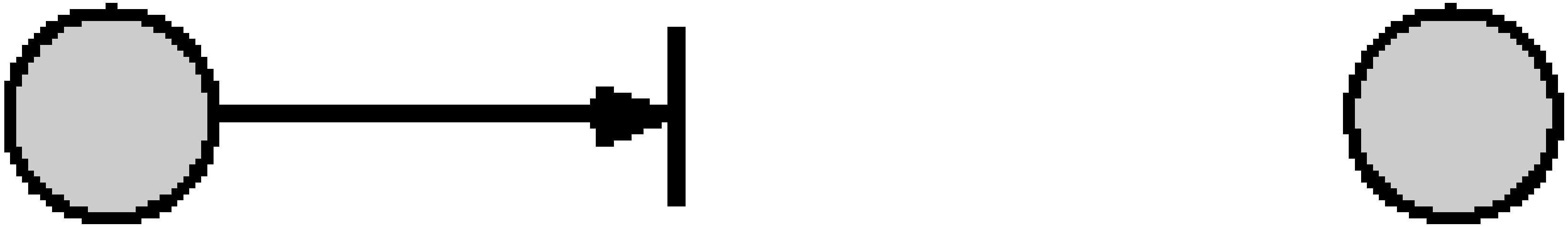


(c) Interception

Interruption (Jamming)

- The action of preventing a message from reaching its intended recipient.
- An asset of the system is destroyed or becomes unavailable or unusable.
- This is an attack on the availability. An asset of a system becomes unavailable.
- Examples include
  - destruction of a piece of hardware, such as a hard disk,
  - The attacker may cut the communication link or use jamming to interrupt wireless communications,
  - The disabling of the file management system, or
  - injecting a huge amount of data to a specific target
- **DOS** - Denial of Service Attacks have become very well known.

Interruption



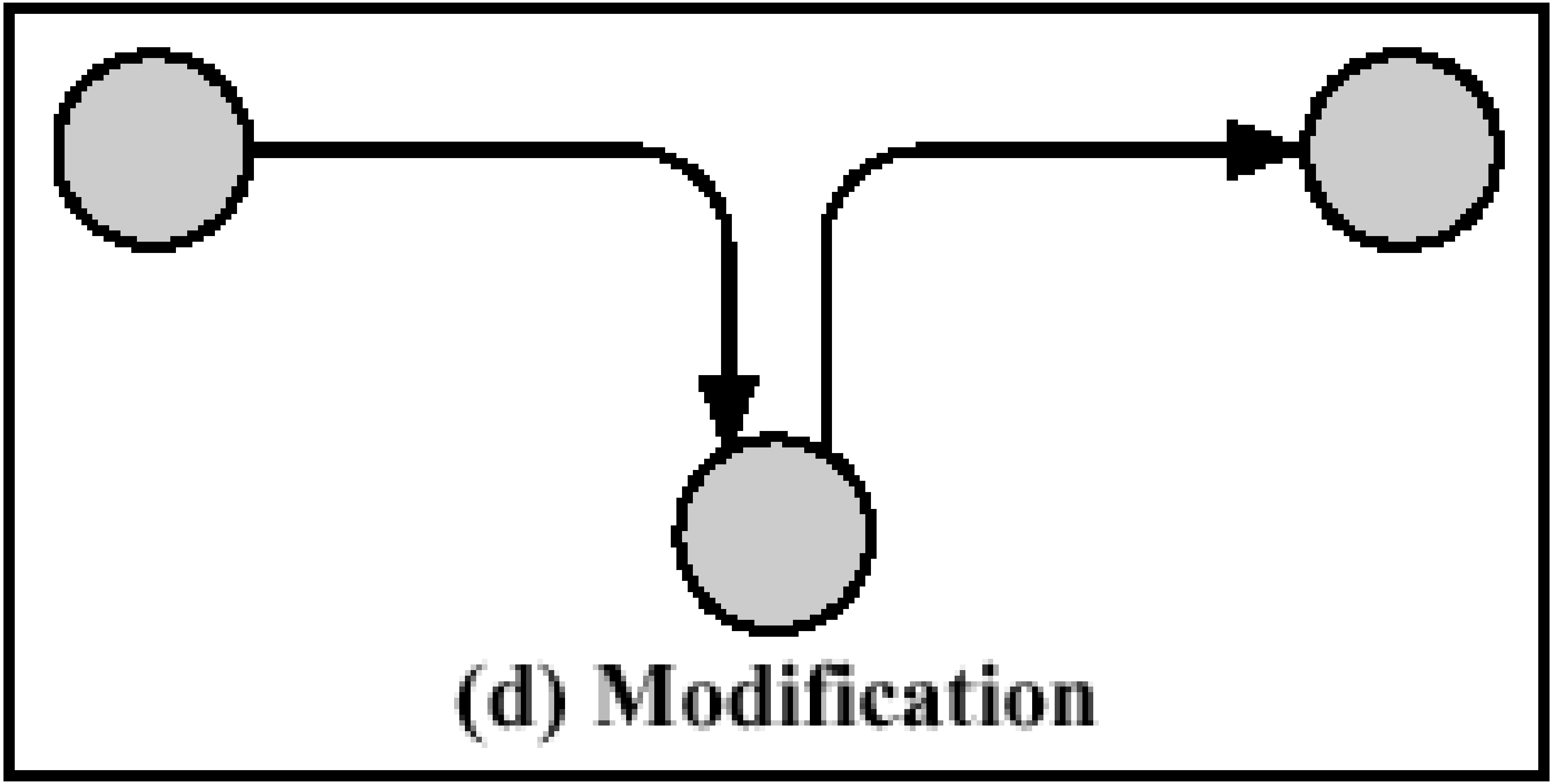
(b) Interruption

Modification (tampering)

- An unauthorized party not only gains access to but tampers with an asset.
- An unauthorised party alters the content of a message which is transmitted between entities. In other words, the information is altered and then sent to the recipient.
- Modification is integrity violation.
- This is an attack on the integrity like changing the content of message being transmitted
- Examples include changing values in a data file, altering a program so that it performs differently, and modifying the content of a message being transmitted in a network.
- The countermeasure against this attack is cryptographic technique

  (checksums or digital signature).

Modification (tampering)

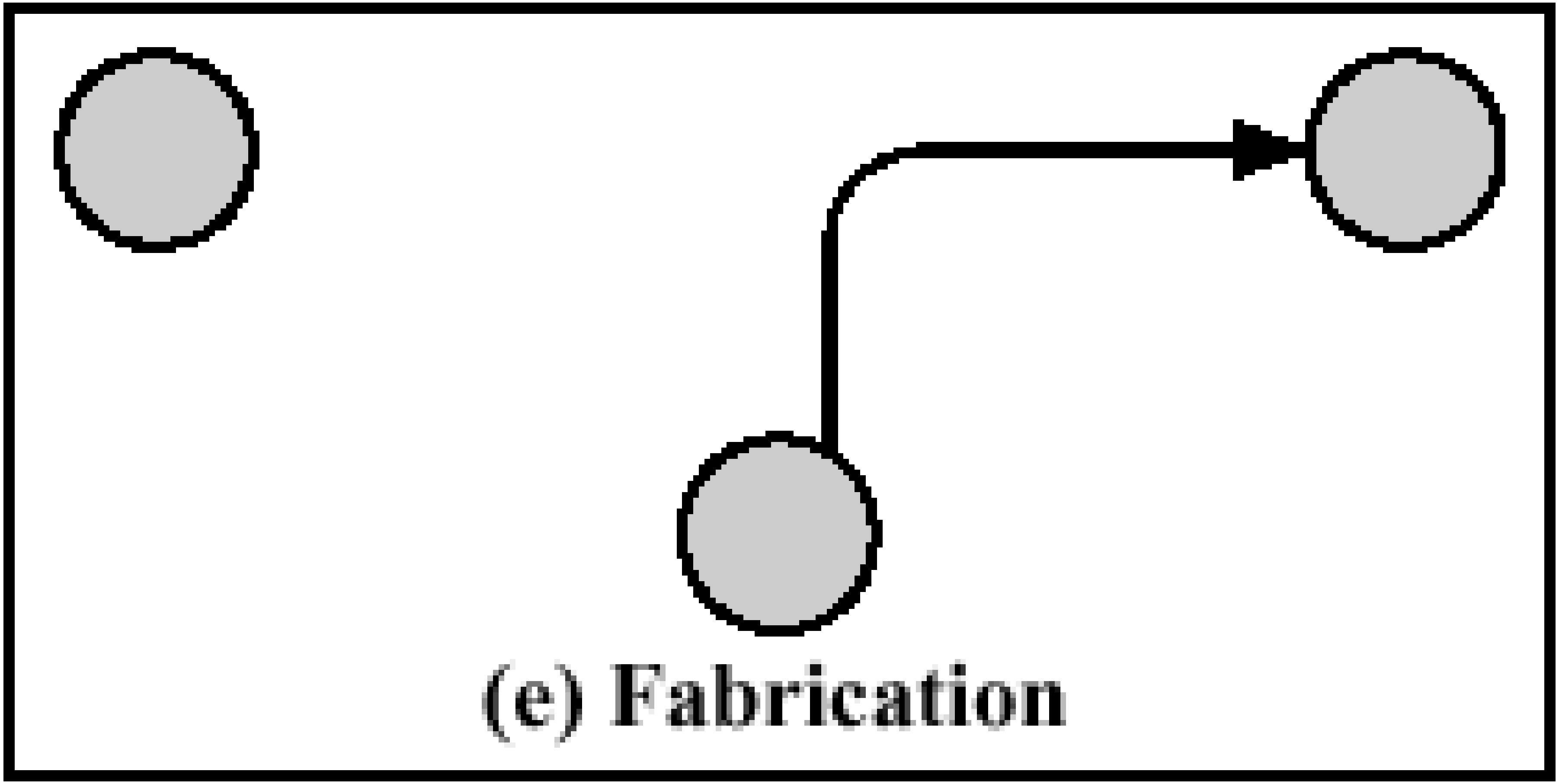


(d) Modification

Fabrication (Impersonation)

- An unauthorized party inserts counterfeit objects into the system.
- This is an attack on the authenticity.
- Allows to bypass (avoid) the authenticity check.
- Examples include the insertion of spurious messages in a network, the addition of records to a file or counterfeit bank notes, fake cheques,
- The countermeasure against this attack is cryptographic technique.

Fabrication (Impersonation)



Vulnerabilities, Threats and Attacks

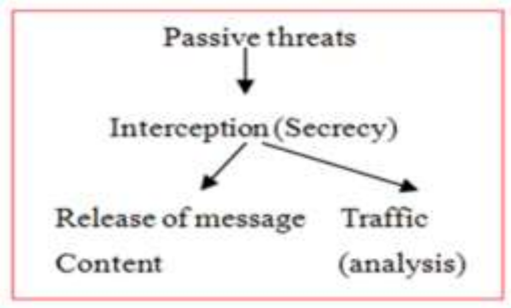
- Categories of vulnerabilities
  - Corrupted (loss of integrity)
  - Leaky (loss of confidentiality): For example, someone who should not have access to some or all of the information available through the network obtains such access.
  - Unavailable or very slow (loss of availability)
- Threats
  - Capable of exploiting vulnerabilities
  - Represent potential security harm to an asset
- Attacks (threats carried out)
  - Passive – attempt to learn or make use of information from the system that does not affect system resources
  - Active – attempt to alter system resources or affect their operation
  - Insider – initiated by an entity inside the security parameter
  - Outsider – initiated from outside the perimeter

Table 1.2 Threat Consequences, and the Types of Threat Actions That Cause Each Consequence. Based on RFC 2828

Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure A situation or event whereby an entity gains access to data for which the entity is not authorized. **It is Threat to Confidentiality**	**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 avoiding a system's security protections.
Deception (Cheat) A situation or event that may result in an authorized entity receiving false data and believing it to be true. **It is Threat to Inegrity**	**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 situation or event that interrupts or prevents the correct operation of system services and functions. **It is Threat to Avalibility**	**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 situation or event that results in control of system services or functions by an unauthorized entity. **It is Threat to Integrity**	**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.

Network Security Attacks

- Two types of **passive attacks** are:
  - Release of message contents and
  - Traffic analysis.



Passive threats

Interception (Secrecy)

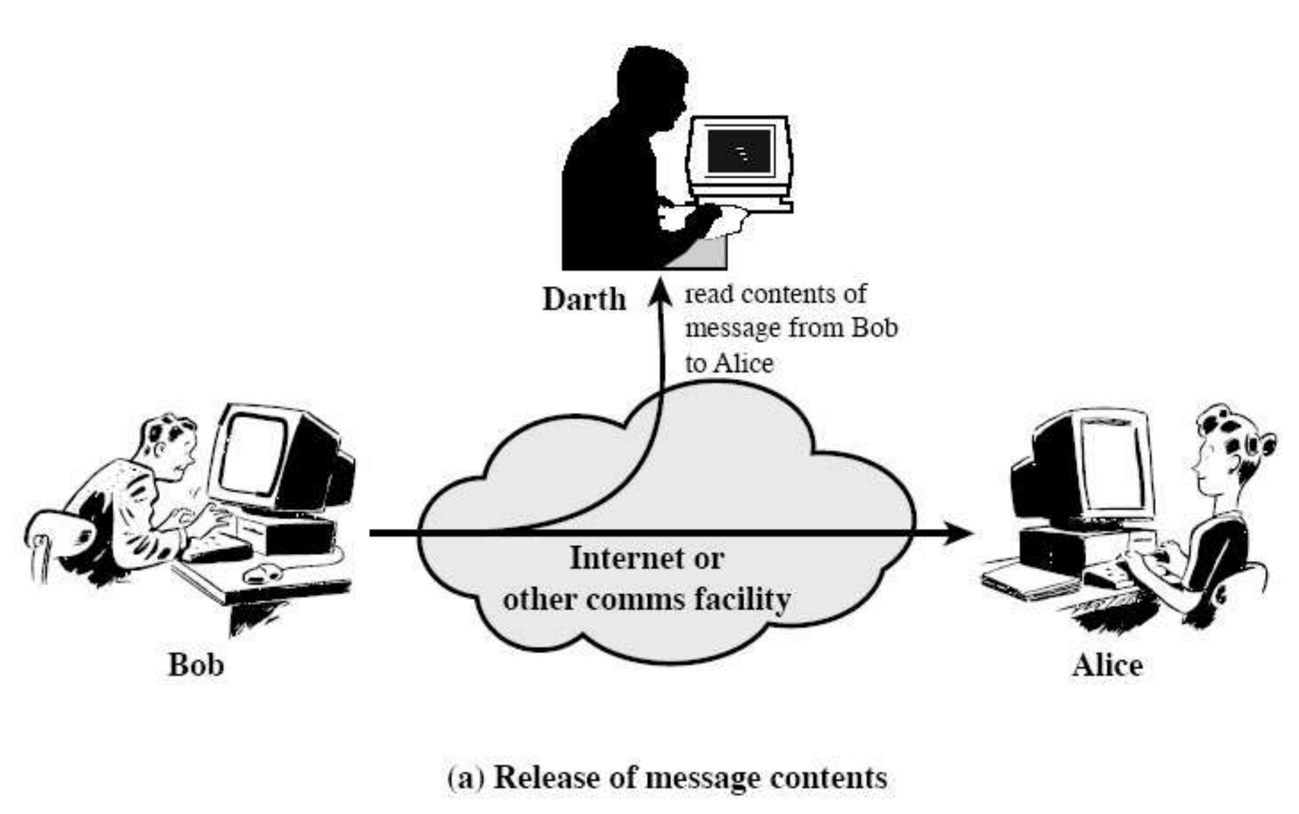
Release of message Content

Traffic (analysis)

- **Release of message contents.**
  - A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.
- **Traffic analysis .**
  - Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Passive Attacks

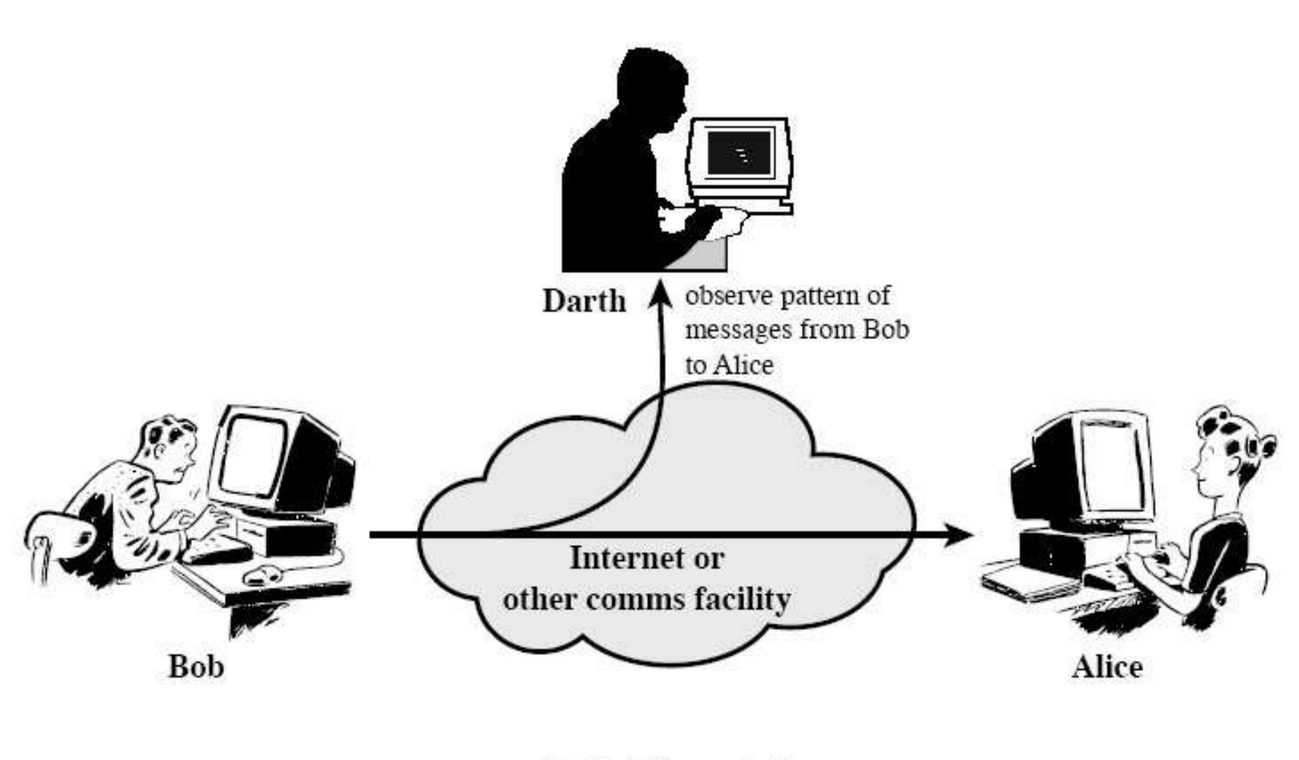
- Release of message contents
  - Telephone conversation tapping, interception of emails or file transferred.


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

(a) Release of message contents

Passive Attacks (cont'd)

- Traffic Analysis
  - Intercept an encrypted message and try to decrypt it


Darth
observe pattern of messages from Bob to Alice
Bob
Internet or other comms facility
Alice

(b) Traffic analysis

Network Security Attacks

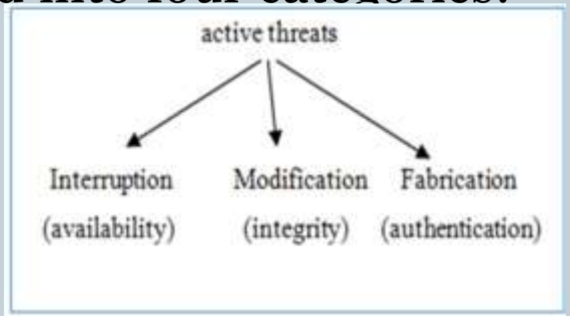
- **Passive attacks** are very difficult to detect because they do not involve any alteration of the data.
- Typically, the message traffic is sent and received in an apparently normal fashion and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of encryption.
- Thus, the emphasis in dealing with passive attacks is on **prevention rather than detection.**

Network Security Attacks

- Active Attacks
  - Involve modification of the data stream or creation of a false stream
  - E.g. Masquerade, replay, message modification, denial of services
  - Potentially detected by security mechanisms
  - Replay, Interruption, Modification, Fabrication

Network Security Attacks

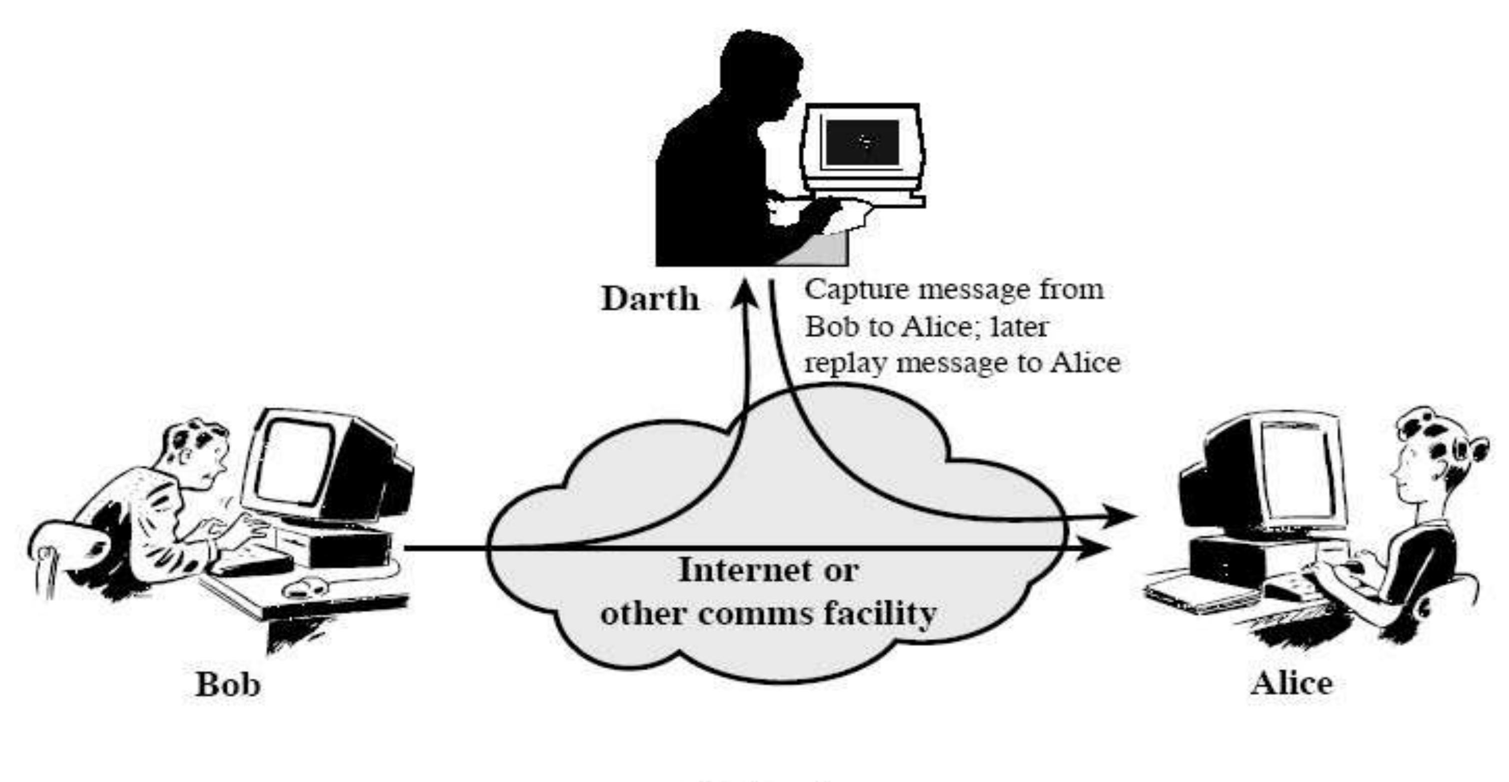
- **Active attacks** involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories:
  - Replay
  - Masquerade,
  - Modification of messages
  - Denial of service.



- **Replay:** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- **A masquerade:** takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

Active Attacks (cont'd)

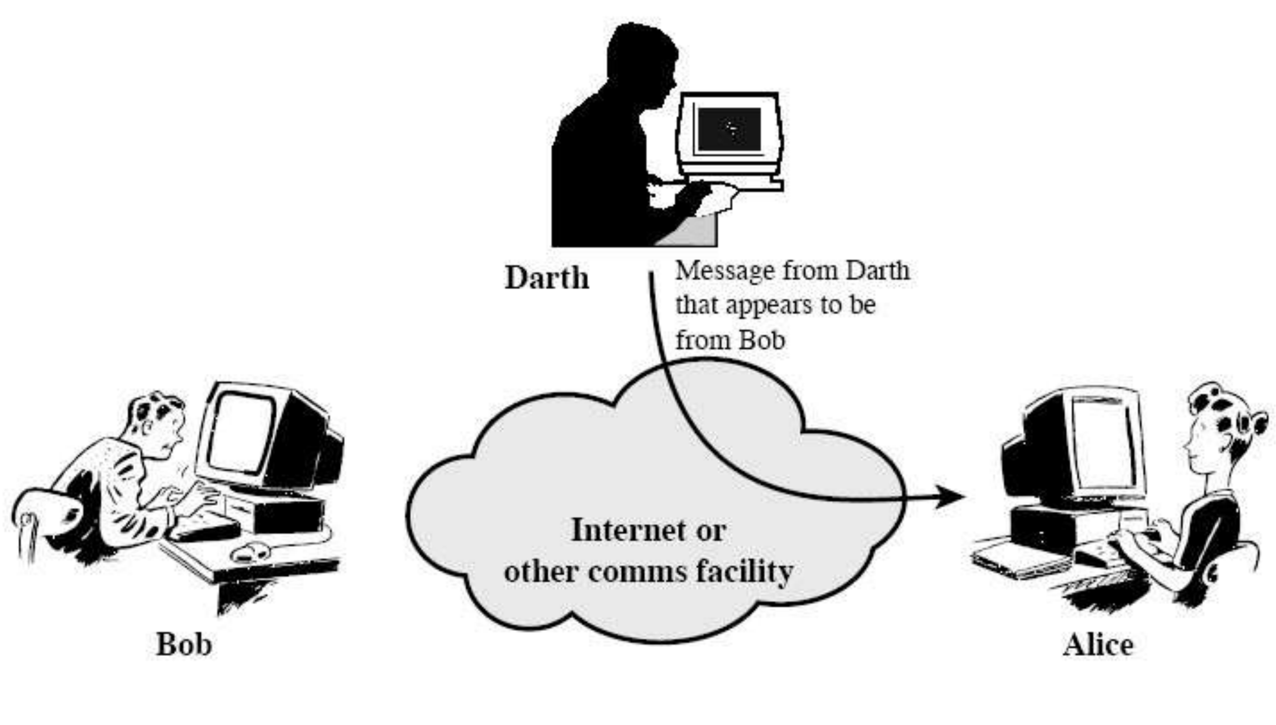
- **Replay**
  - Intercept -> Replay -> Masquerade


Darth
Capture message from Bob to Alice; later replay message to Alice
Bob
Internet or other comms facility
Alice

(b) Replay

Active Attacks

- **Masquerade**
  - Pretending to be an authorized party.



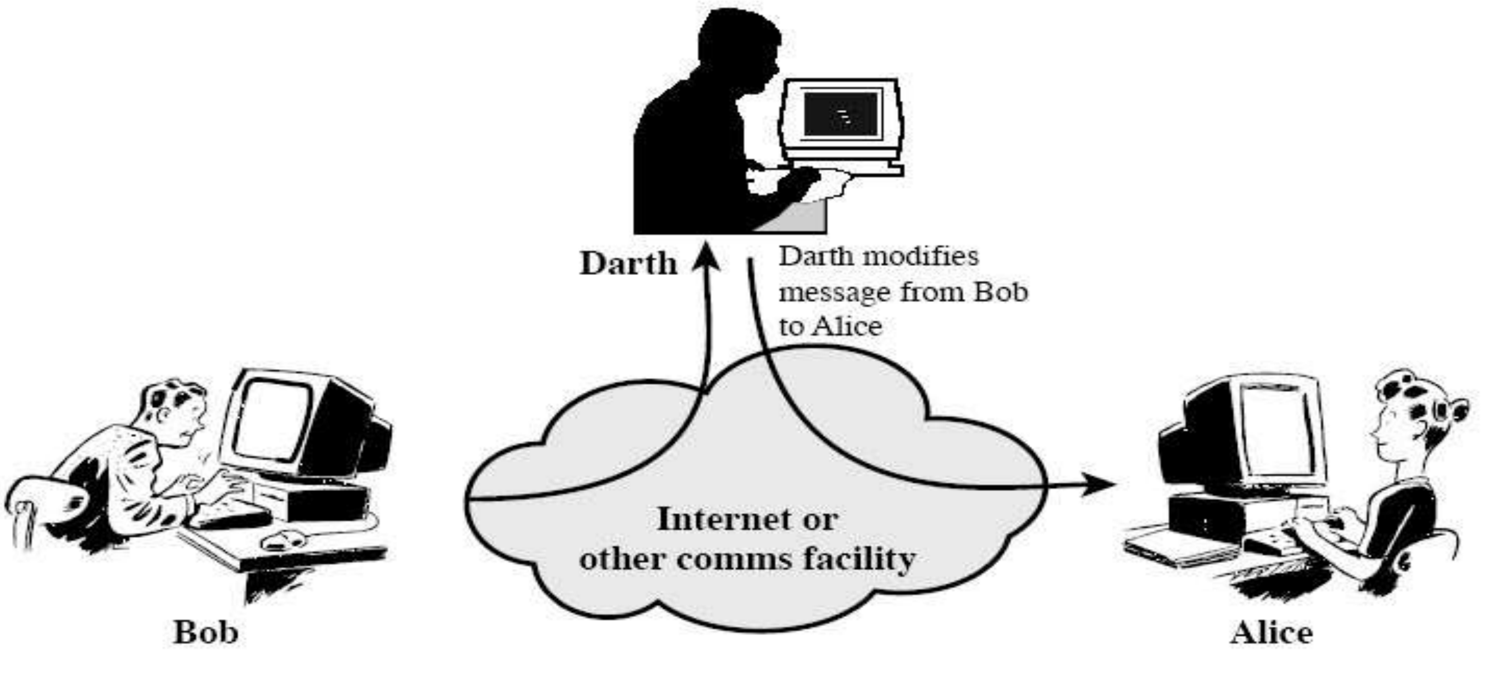
(a) Masquerade

Network Security Attacks

- **Active attacks** can be subdivided into four categories:
  - Replay
  - Masquerade,
  - Modification of messages
  - Denial of service.
- **Modification of messages** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. For example, a message stating, “Allow Yousef to read confidential file accounts” is modified to say, “Allow Dana to read confidential file accounts.”
- The **denial of service** prevents the normal use or management of communications facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

Active Attacks (cont'd)

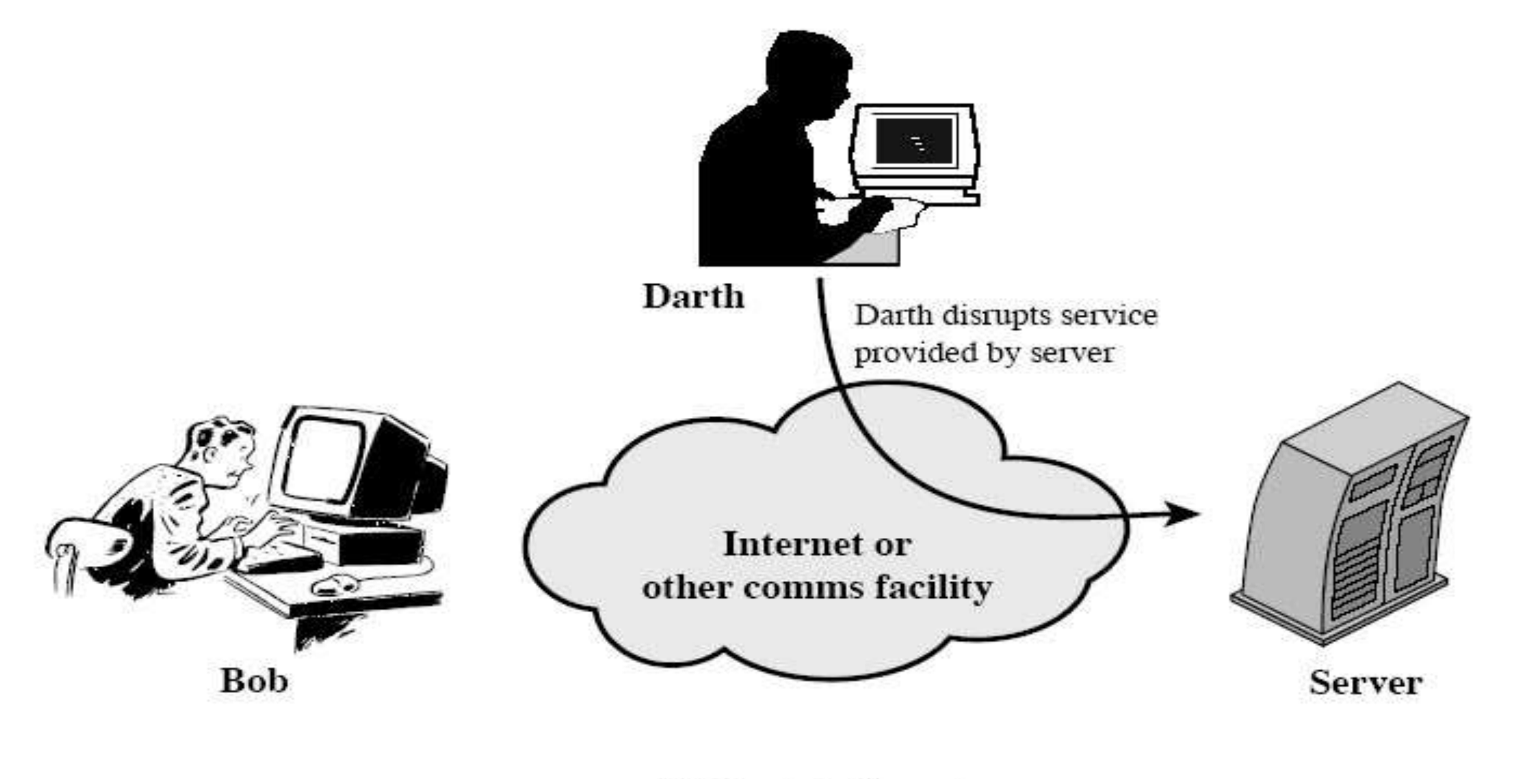
- **Modification of messages**
  - Modify content of a message to produce unauthorized effect


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

(c) Modification of messages

Active Attacks (cont'd)

- **Denial of Service**
  - An attempt to stop a system to provide services

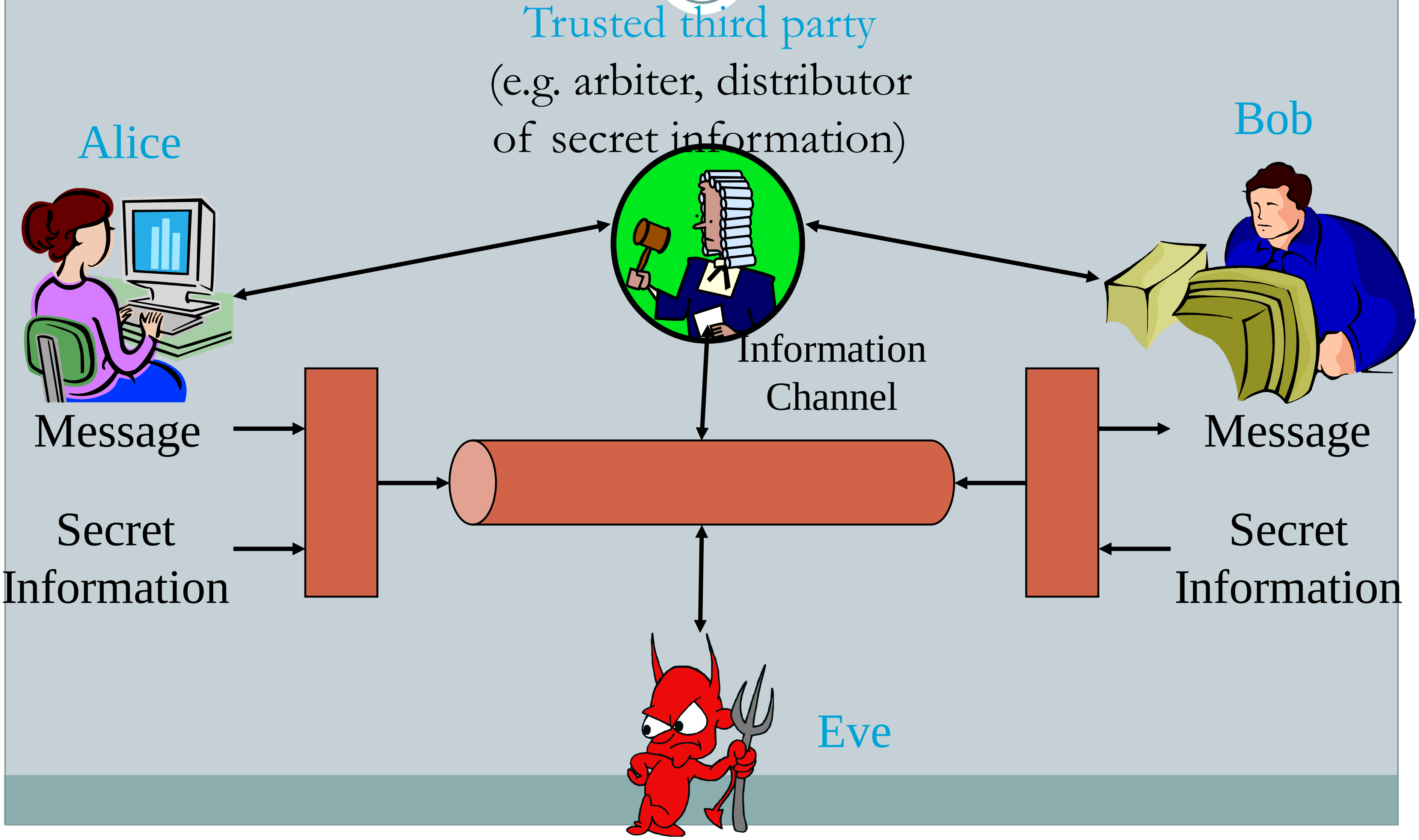

Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

(d) Denial of service

Attacks

- We can also classify attacks based on the origin of the attack:
  - 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").

Model for Network Security



Model for Network Security

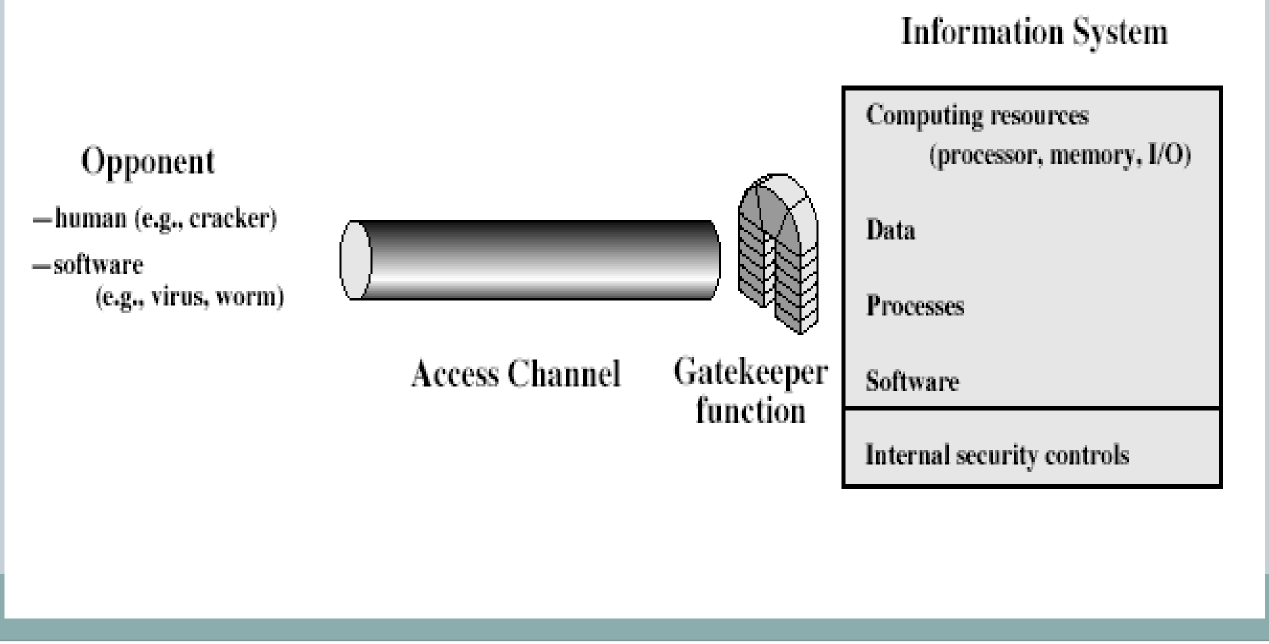
- The General model shows that there are four basic tasks in this design:
  - Algorithm: for performing the security related transformation. The algorithm should be designed in such a way that an opponent can not defeat its purpose.
  - Generate the secret information – Keys: to be used with the aid of an algorithm.
  - Distribution and sharing of the secret information.
  - Specify a protocol: to be used by the two principals that make use of the secrecy algorithm and the secret information to achieve a particular security service.

Network Access Security Model

- Hacker
  - The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system.
- Intruder
  - The intruder can be a disgruntled employee who wishes to do damage or a criminal who seeks to exploit computer assets for financial gain (e.g., obtaining credit card numbers or performing illegal money transfers).

Network Access Security Model

- The below figure shows the general access model. It is suitable for protection against unauthorized or unwanted access.
- Two broad categories of security measures:
  - A gatekeeper function. It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic.
  - Internal controls that monitor activity and analyze stored information in an attempt to detect the unwanted intruders as a second line of defense.



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.

Security Requirements

- **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.

Security Requirements

- **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 (penalty, punishment)for personnel failing to comply with organizational security policies and procedures.

Security Requirements

- **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 (qain):** (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.

Fundamental Security Design Principles

- The following as fundamental security design
  - Economy of mechanism
  - Fail-safe defaults
  - Complete mediation
  - Open design
  - Separation of privilege
  - Least privilege
  - Least common mechanism
  - Psychological acceptability
  - Isolation
  - Encapsulation
  - Modularity
  - Layering

Fundamental Security Design Principles

- **Economy of mechanism** means that the design of security measures embodied in both hardware and software should be as simple and small as possible.
- **Fail-safe default** means that access decisions should be based on permission rather than exclusion. For example, most file access systems work on this principle and virtually all protected services on client/server systems work this way.
- **Complete mediation** means that every access must be checked against the access control mechanism. Systems should not rely on access decisions retrieved from a cache. In a system designed to operate continuously, this principle requires that, if access decisions are remembered for future use, careful consideration be given to how changes in authority are propagated into such local memories. File access systems appear to provide an example of a system that complies with this principle. However, typically, once a user has opened a file, no check is made to see of permissions change. To fully implement complete mediation, every time a user reads a field or record in a file, or a data item in a database, the system must exercise access control.

Fundamental Security Design Principles

- **Open design** means that the design of a security mechanism should be open rather than secret. For example, although encryption keys must be secret, encryption algorithms should be open to public study.
- **Separation of privilege** is defined in [SALT75] as a practice in which multiple privilege attributes are required to achieve access to a restricted resource. A good example of this is multifactor user authentication, which requires the use of multiple techniques, such as a password and a smart card, to authorize a user.
- **Least privilege** means that every process and every user of the system should operate using the least set of privileges necessary to perform the task.
- **Least common mechanism** means that the design should minimize the functions shared by different users, providing mutual security. This principle helps reduce the number of unintended communication paths and reduces the amount of hardware and software on which all users depend, thus making it easier to verify if there are any undesirable security implications.

Fundamental Security Design Principles

- **Isolation** is a principle that applies in three contexts. First, public access systems should be isolated from critical resources (data, processes, etc.) to prevent disclosure. Second, the processes and files of individual users should be isolated from one another except where it is explicitly desired. All modern operating systems provide facilities for such isolation, so that individual users have separate, isolated process space, memory space, and file space, with protections for preventing unauthorized access. And finally, security mechanisms should be isolated in the sense of preventing access to those mechanisms.
- **Encapsulation** can be viewed as a specific form of isolation based on object oriented functionality. Protection is provided by encapsulating a collection of procedures and data objects 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.

Fundamental Security Design Principles

- **Modularity** in the context of security refers both to the development of security functions as separate, protected modules and to the use of a modular architecture for mechanism design and implementation.
- **Layering** refers to the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems. By using multiple, overlapping protection approaches, the failure or of any individual protection approach will not leave the system unprotected.

Summary

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

- Fundamental security design principles