Chapter-1

Introduction to Computer Security (5 Hours)

Chapter Outlines

- Basic Components of Security
- Security Threats
- Issues with Security
- Security Policies
- Types of Security Policy
- Access Control
- Type of Access Control
- Overview of the Bell-LaPadula Model and Biba Integrity Model

Thoughts of

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have our position unassailable.

- The Art of War, Sun Tzu

Background

- ***Information security*** was provided, before digital age, in an organization by physical and administrative means e.g. Filing cabinet with locking system, personnel screening at the time of recruitment etc.
- With the introduction of computers, and development of shared systems, public telephone networks, data networks and the internet, the term ***Computer security*** was defined as "*A collection of tools designed to protect data and to thwart hackers.*"
- Distributed systems and the use of network and communications facilities give rise to the need of security measures to protect data during their transmission, and hence the term ***Network security*** was introduced.
- Nowadays, most organizations interconnect their data processing equipment's with inter-connected networks (i.e. internet). So, the term ***internet security*** is used.

Security Violation: Scenario 1

- User A transmits a file to user B. The file contains sensitive information (e.g., payroll records) that is to be protected from disclosure. User C, who is not authorized to read the file, is able to monitor the transmission and capture a copy of the file during its transmission.

Security Violation: Scenario 2

- A network manager, D, transmits a message to a computer, E, under its management. The message instructs computer E to update an authorization file to include the identities of a number of new users who are to be given access to that computer. User F intercepts the message, alters its contents to add or delete entries, and then forwards the message to E, which accepts the message as coming from manager D and updates its authorization file accordingly.

Security Violation: Scenario 3

- Rather than intercept a message, user F constructs its own message with the desired entries and transmits that message to E as if it had come from manager D. Computer E accepts the message as coming from manager D and updates its authorization file accordingly.

Security Violation: Scenario 4

- An employee is fired without warning. The personnel manager sends a message to a server system to invalidate the employee’s account. When the invalidation is accomplished, the server is to post a notice to the employee’s file as confirmation of the action. The employee is able to intercept the message and delay it long enough to make a final access to the server to retrieve sensitive information. The message is then forwarded, the action taken, and the confirmation posted. The employee’s action may go unnoticed for some considerable time.

Security Violation: Scenario 5

- A message is sent from a customer to a stockbroker with instructions for various transactions. Subsequently, the investments lose value and the customer denies sending the message.

Definition: Computer Security

- The NIST (National Institute of Standards and Technology) *Computer Security Handbook*[NIST95] 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).

- This definition includes three key objectives that are at the heart of computer security.
  - **Confidentiality**
  - **Integrity**
  - **Availability**

- These three concepts form what is often referred to as **CIA triad**.

The CIA Triad: Confidentiality

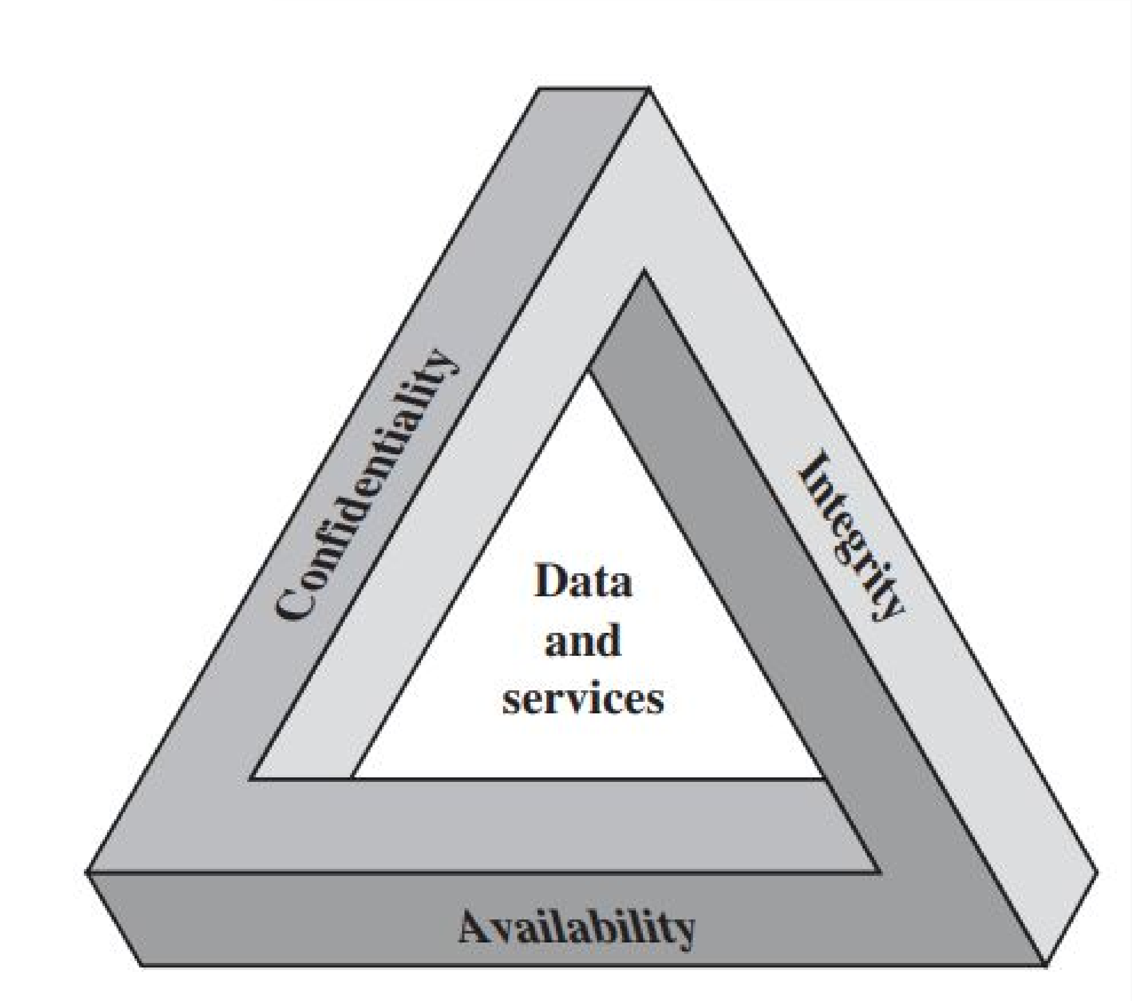
- **Confidentiality**:
- *Confidentialtiy* is the concealment of information of resources.
- This term covers two related concepts:
  - **Data confidentiality**: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
  - **Privacy**: Assures that 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

The CIA Triad: Integrity

- **Integrity**:
- Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change.
- 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 manner, free from deliberate or inadvertent unauthorized manipulation of the system.

The CIA Triad: Availability

- **Availability**:
- *Availability* refes to the ability to use the information or resource desired.
- Assures that systems work promptly and service is not denied to authorized users.



The CIA Triad: Security Characteristics

FIPS 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category

- 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.

- 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.

Additional concepts for complete picture

- Authenticity
  - The property of being genuine and being able to be verified and trusted.
  - Authenticity is assurance that a message, transaction, or other exchnage is from source it claims to be from, i.e. proof of identity.

- Accountability

  - It means that every individual who works with an information system should have specific responsibilities for information assurance.

The OSI Security Architecture

- The ITU-T (International Telecommunication Union Telecommunication Standardization Sector) Recommendation X.800, ***Security Architecture for OSI***, gives structured definition of security attacks, security mechanism and security services.
- **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. Examples: encipherment, digital signature, access control etc.
- **Security service**: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service. It includes authentication, access control, data confidentiality, data integrity and non-repudiation.

Security Threats

- A threat is a potential violation of security which might or might not occur.
- The fact that the violation *might* occur means that those actions that could cause it to occur must be guarded against (or prepared for).
- Those actions are called *attacks*.
- Those who execute such actions, or cause them to be executed, are called *attackers*.

Security Threats

- Security Threats divided into four broad classes:

I. **Disclosure**, *an unauthorized access to information*

II. **Deception**, an *acceptance of false data*

III. **Disruption**, an *interruption of prevention of correct information*

IV. **Usurpation**, an *unauthorized control to some part of a system*

The OSI Security Architecture

According to 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 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.
- In literature, however, they are commonly mean more or less the same thing.

Security Attack

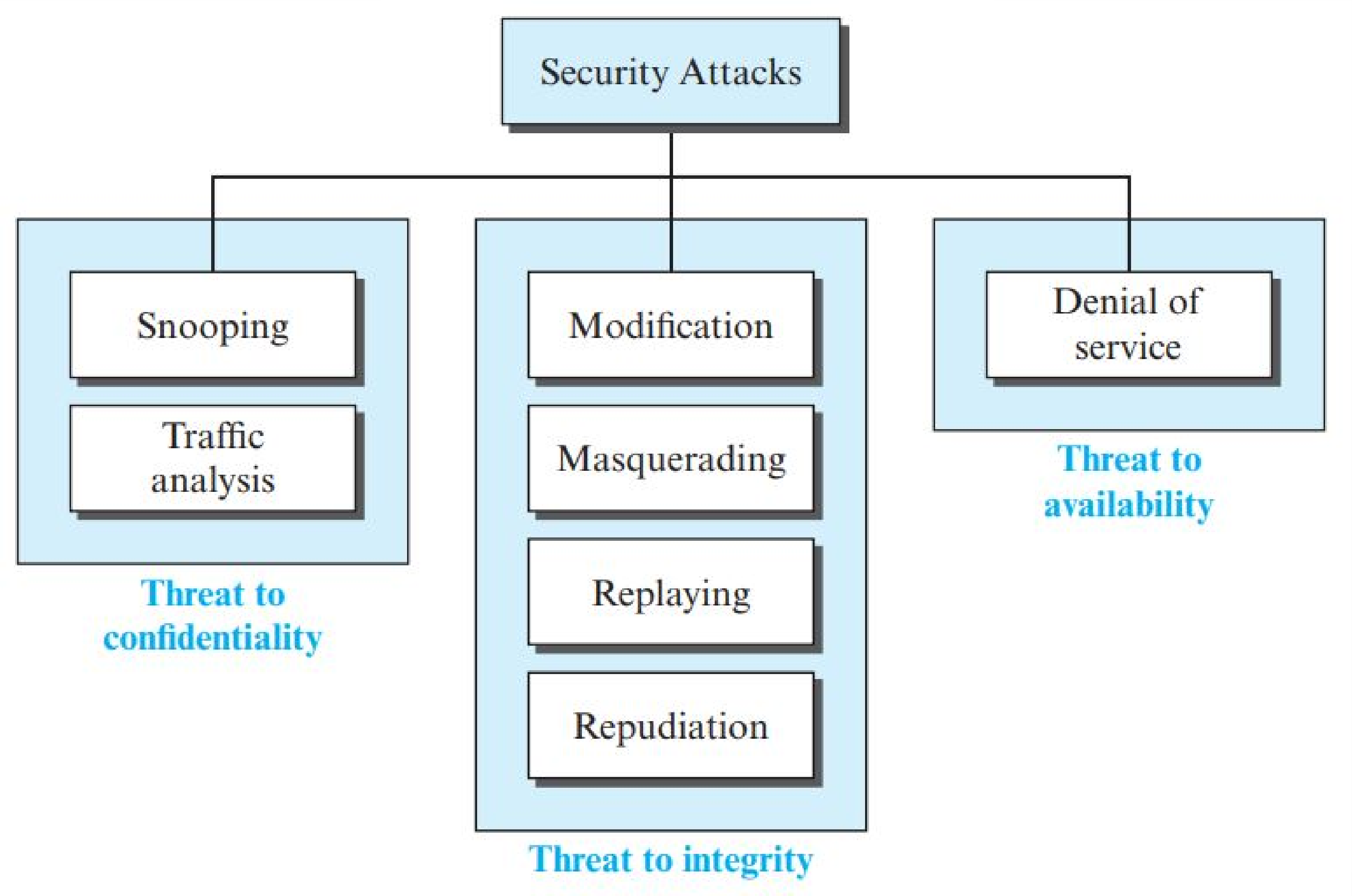
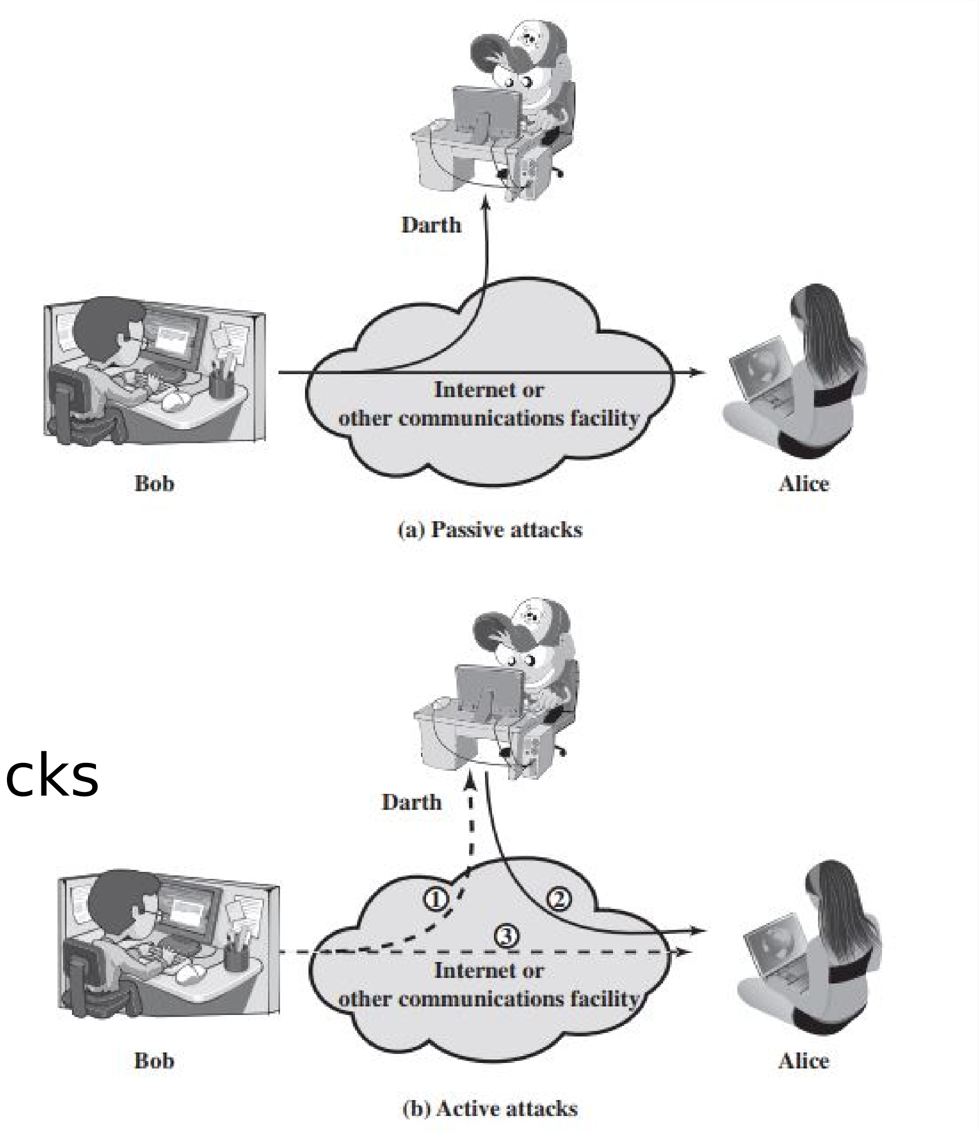


Figure: Taxonomy of attacks with relation to security goals.

Security Attacks

- Security attacks are classified as:
  1. Passive Attacks
  2. Active Attacks



(a) Passive attacks

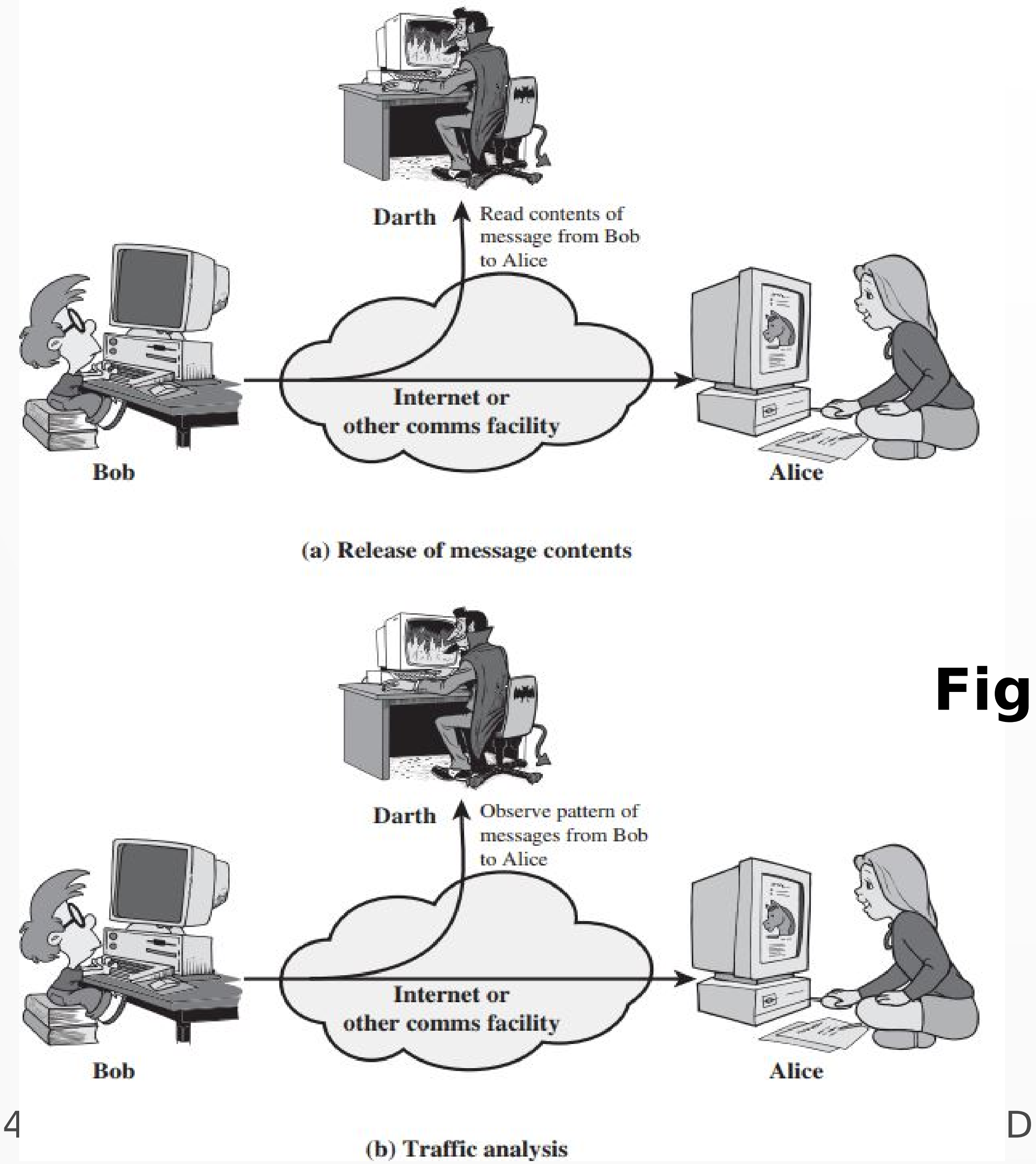
(b) Active attacks

Figure: Security Attacks

Security Attacks: Passive

- Passive attack attempts to learn or make use of information from the system but does not affect system resources.
- Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.
- Two types:
  1) The release of message
  2) Traffic analysis
- Passive attacks are very difficult to detect, because they do not involve any alternation of the data.
- But it is feasible to prevent by means of encryption.

Security Attacks: Passive


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

(a) Release of message contents

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

(b) Traffic analysis

Figure: Passive network security attacks.

Security Attacks: Active

- Active attacks attempt to alter system resources or affect their position.
- It involves some modification of the data stream or the creating of a false stream.
- Active attacks are quite difficult to be absolutely prevented because of the wide variety of potential physical, software, and network vulnerabilities.
- Examples of active attacks are:

  - Masquerade
  - Replay
  - Modification of messages,
  - Denial of service, etc.

Snooping

- *Snooping* refers to unauthorized access to or interception of data. It is a form of disclosure.
- Wiretapping is a form of snooping in which a network is monitored.
- For example, a file transferred through the Internet may contain confidential information. An unauthorized entity may intercept the transmission and use the contents for her own benefit.

Traffic Analysis

- Unauthorized access to information by observing the monitoring online traffic.
- For example: observing and collecting the email address, nature of transactions etc.

Modification

- 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.
- It is an active security attack in which unauthorized change of information is done by ‘Man-in the Middle’.
- For example, a message meaning “Allow John Smith to read confidential file accounts” is modified to mean “Allow Fred Brown to read confidential file accounts.”

Masquerade or Spoofing

- Masquerade takes place when the attacker impersonate somebody else.
- It is a form of deception and usurpation.
- If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack.
- For example: gaining access to the account of a legitimate user either by stealing the victim's account ID and password.
- Similarly, if a user tries to read a file, but an attacker has arragned for the user to be given a different file, another spoof has taken place.

Replay

- Replay involves the passive capture of a data unit and its subsequent re-transmission to produce an unauthorized effect.

Repudiation

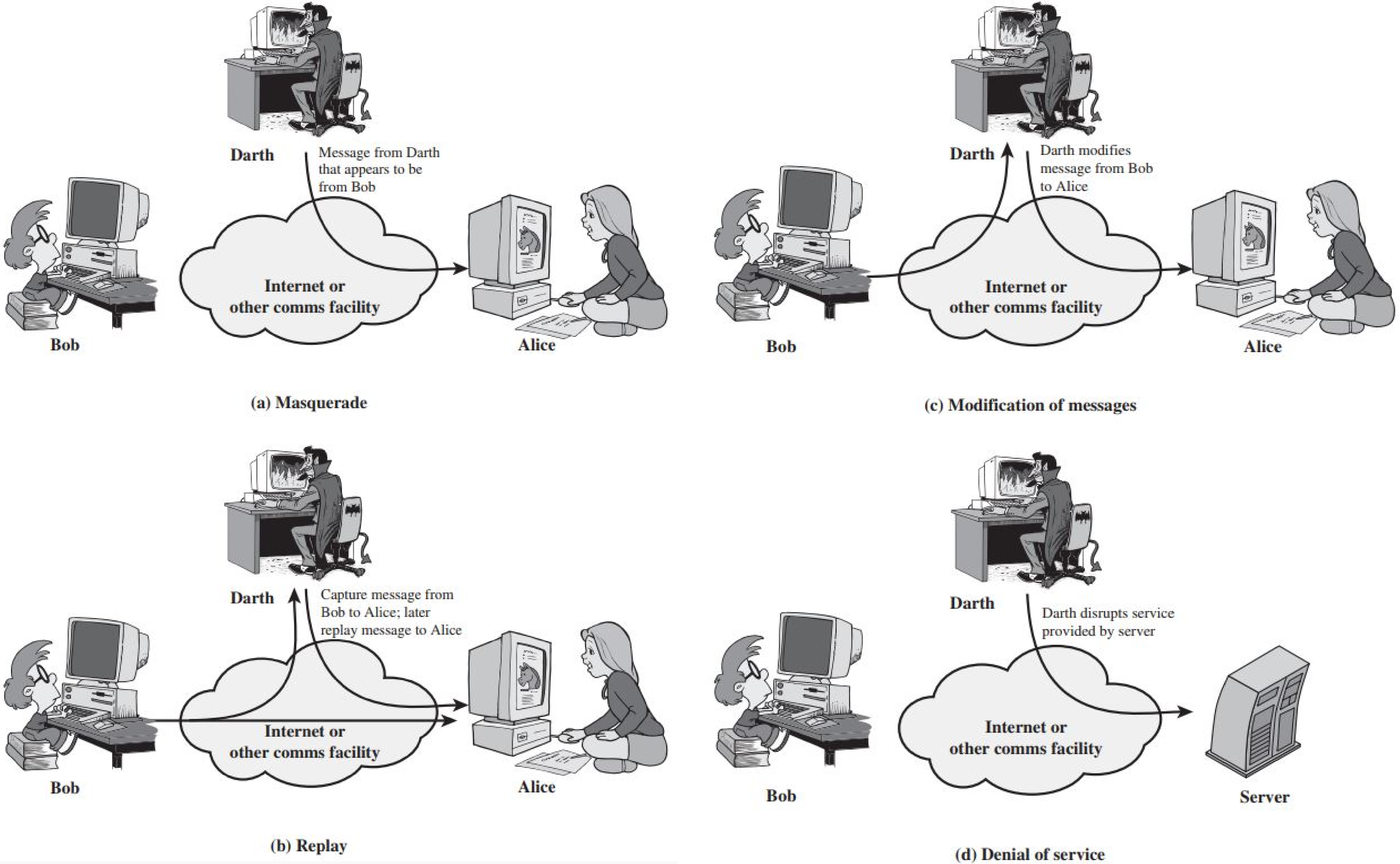
- This type of attack is different from others because it is performed by one of the two parties in the communication: the sender or the receiver.
- The sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.
- It is a form of deception.

Delay

- Typically, delivery of a message or service requires some time *t*;
- If an attacker can force the delivery to take more than time t, the attacker has successfully delayed delivery.
- This involves the manipulation of system control structures, such as network components or server components, and hence a form of usurpation.

Denial of Service

- The denial of service prevents or inhibits 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.
- Denial of Service poses the same threat as an infinite delay.


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice
Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice
Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice
Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

(a) Masquerade

(c) Modification of messages

(b) Replay

(d) Denial of service

Issues and Challenges of Computer Security

- Providing security is not as easy as it seems to be. The requirements for providing security (confidentiality, authentication, integrity) are quite complex, and understanding them involves complex reasoning.
- In developing a particular security mechanism or algorithm, potential attacks should be considered. But unexpected attacks may occur.

Issues and Challenges of Computer Security (contd..)

- The procedures used to provide particular are complex. The security mechanism should be updated regularly to adapt to the changes.
- Having designed various security mechanism, it is necessary to decide where to use them: both in terms of physical and logical sense.
- Security mechanisms typically involve more than a particular algorithm or protocol. It also requires the knowledge of system and network.
- Strong security as burden to efficient and user friendly environment and operations.

Issues and Challenges of Computer Security (contd..)

- Computer and Network Security is a battle between the intruder and the designer and administrator.
- The users or system managers hesitate to invest on security due to little benefits until a security failure occurs.
- Security requires regular and constant monitoring which is a difficult in today’s short-term and overloaded environment.
- Security is implemented after the system design rather than a part of the design process.

Operational Issues

- Any useful policy and mechanism must balance the benefits of the protection against the cost of designing, implementing, and using the mechanism.
- This balance can be determined by analyzing the risks of a security breach and the likelihood of it occurring.
- Such an analysis is, to a degree, subjective, because in very few situations can risks be rigorously quantified

Operational Issues

- The Operational Issues are:

I. Cost-benefit analysis

II. Risk Analysis

III. Laws and Customs

-

I. Cost-Benefit Analysis

- The benefits of computer security are weighed against their total cost (including the additional costs incurred if the system is compromised).
- If the data or resources cost less, or are of less value, than their protection, adding security mechanisms and procedures is not cost-effective.
- The cost-benefit analysis should take into account as many mechanisms as possible.
- *For example*: Database of salary information system in banks: main office and branch offices.

ii. Risk Analysis

- To determine whether an asset should be protected, and to what level, requires analysis of the potential threats against that asset.
- The level of protection is a function of the probability of an attack occurring and the effects of the attack could cause the loss.
- Priority should be given to the tasks that have higher importance.
- For example: Protection of network with internet requires higher attention than without the internet.

iii. Laws and Customs

- Any policy and mechanism for security must consider the legal constraints and abide by laws.
- Restrictions affect procedural controls.
- *For example* : Until the year 2000, the United States controlled the export of strong cryptographic hardware and software (considered munitions under United States law). If a U.S. software company worked with a computer manufacturer in London, the U.S. company could not send cryptographic software to the manufacturer. The U.S. company first would have to obtain a license to export the software from the United States. Any security policy that depended on the London manufacturer’s using that cryptographic software would need to take this into account.

Human Issues

- Though computer security is more of technical aspects in large organization, non-technical considerations affect their implementation and use.
- Incorrectly configured or used can affect severely.
- Thus, the designers, implementer, and maintainers of security controls are essential to the correct operation of those controls.
- As a human issues can be:

  a) Organizational problems

  b) People problems

Human Issues

Organizational Problems

- Security limits loss, but it requires expenditure on resources.
- Unless the loss occurs by security breach, organization believes they are wasting effort in security.
- Furthermore, security adds extra complexity to simple operations, which may cause decrease in productivity.
- Losses occur when security protections are in place, but such losses are expected to be less than they would have been without the security mechanisms.
- Many organization face the lack of people trained in the computer security and also they lack needed resources.

Human Issues

People Problems

- The heart of any security system is people. Technological controls depends on human operations.
- There is always risks of human intervention.
- *For example*: computer system authenticates a user by asking a human for a secret code; if the correct secret code is supplied, the computer assumes that the human is the user, and grants the appropriate access. If an authorized user tells another person his secret code, the unauthorized user can masquerade as the authorized user with small risk of detection.
- Insider misuse of authorized privileges, untrained personnel, system administrators misreading the output of security mechanism etc. pose the probability of successful attacks on their system.

Security Policies

- A security policy defines “***secure***” for a system or a set of systems.
- Security policy defines the goals and elements of an organization’s computer systems that specifies what is allowed to do and what is not.
- With respect to confidentiality, a security policy identifies the leakage of information flow.
- With respect to integrity, a security policy identifies authorized ways in which information may be altered and entities authorizes to alter it.
- With respect to availability, a security policy describes what services must be provided.

Security Policies: Definitions

- Consider a computer system to be a finite-state automation with a set of transition functions that change state. Then
- A *security policy* is a statement the partitions the states of the system into a set of *authorized*, or *secure*, states and a set of *unauthorized*, or *non-secure* states.
- A *secure system* is a system that starts in an authorized state and cannot enter an unauthorized state.
- A *breach of security* occurs when a system enters an unauthorized state.

Security Policies: Definition

Consider the finite-state machine in Figure below. It consists of four states and five transitions. The security policy partitions the states into a set of authorized states A = {s_1 , s_2 } and a set of unauthorized states UA = {s_3 , s_4}. This system is not secure, because regardless of which authorized state it starts in, it can enter an unauthorized state. However, if the edge from s_1 to s_3 were not present, the system would be secure, because it could not enter an unauthorized state from an authorized state.

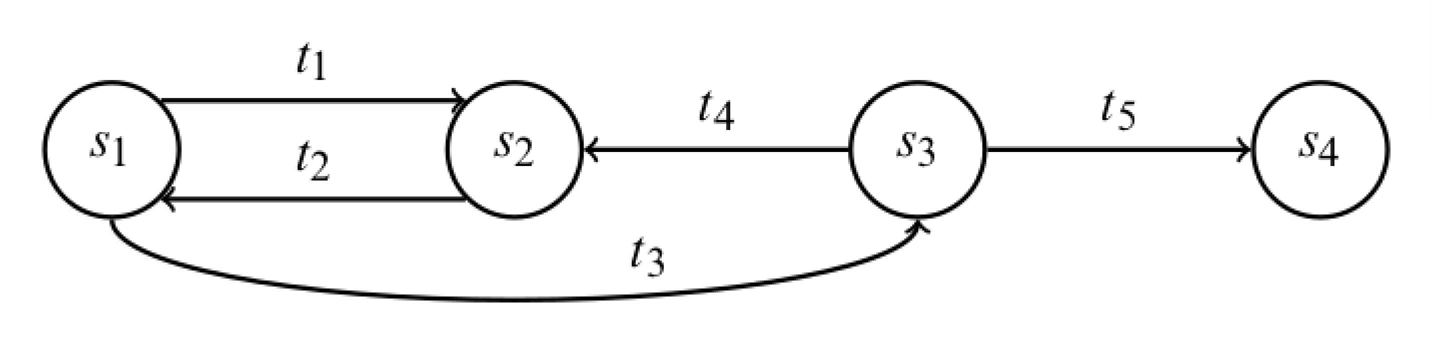


Figure: A simple finite-state machine. In this example, the authorized states are s_1 *and* s_2.

Security Policies: Definition

- A *security mechanism* is an entity or procedure that enforces some part of the security policy.
- A *security model* is a model that represents a particular policy of set of policies.

Types of Policies

1. Military Security Policy or Governmental Security Policy
2. Commercial Security Policy
3. Confidentiality Policy
4. Integrity Policy

1. Military Security Policy or Governmental Security Policy

- Developed to provide confidentiality.
- The name comes from military’s need to keep information (such as date the troop will sail) secret.
- Confidentiality is one of the primary concerns in governmental agencies. Unauthorized disclosure can result in penalties that include jail or fines
- The compromise of confidentiality would be catastrophic, because an opponent would be able to plan countermeasures.

2. Commercial Security Policy

- A *commercial security policy* is a security policy developed primarily to provide integrity.
- The name comes from the need of commercial firms to prevent tampering with their data, because they could not survive such compromises.
- For example, if the confidentiality of a bank's computer is compromised, a customer's account balance may be revealed. This would certainly embarrass the bank and possibly cause the customer to take her business elsewhere. But the loss to the bank's "bottom line" would be minor. However, if the integrity of the computer holding the accounts were compromised, the balances in the customers' accounts could be altered, with financially ruinous effects.

3. Confidentiality Policy

- A *confidentiality policy* is a security policy dealing with confidentiality.
- Both confidentiality policies and military policies deal with confidentiality. However, a confidentiality policy does not deal with integrity at all, whereas a military policy may.
- It is also called an *information flow policy*; prevents the unauthorized disclosure of information.

4. Integrity Policy

- An integrity policy is a security policy dealing only with integrity.
- Commercial policy may deal with confidentiality also but integrity policy does not.

Access Control

- Access control is a security technique that can be used to regulate who or what can view or use resources in a computing environment.
- Access control is a way of limiting access to system or to physical or virtual resources. In computing, access control is a process by which users are granted access and certain privileges to systems, resources or information.

Type of Access Control

1. Discretionary Access Control (DAC)
2. Mandatory Access Control (MAC)
3. Originator Controlled Access Control (ORCON)

1. Discretionary Access Control

- If an individual user can set an access control mechanism to allow or deny access to an object, that mechanism is a *discretionary access control* (DAC), also called an *identity-based access control* (IBAC).
- DAC mechanism controls are defined by user identification with supplied credentials during authentication, such as username and password.

1. Discretionary Access Control (contd..)

- DACs are discretionary because the subject (owner) can transfer authenticated objects or information access to other users.
- In other words, the owner determines object access privileges or an objects access policy is determined by its owner.
- A typical example of DAC is Unix file mode, which defines the read, write an execute permissions.

2. Mandatory Access Control

- When a system mechanism controls access to an object and an individual user cannot alter that access, the control is a *mandatory access control* (MAC), occasionally called a *rule-based access control*.
- The operating system enforces mandatory access controls.
- Each user and device on the system is assigned a similar access.
- When a person or device tries to access a specific resource, the OS checks the entity's credentials to determine whether access will be granted.
- Rules describe the conditions under which access is allowed.

3. Originator Controlled Access Control

- An *originator controlled access control* (ORCON or ORGCON) bases access on the creator of an object (or the information it contains).
- The goal of this control is to allow the originator of the file (or of the information it contains) to control the dissemination of the information.
- Information is controlled by originator or creator of information not owner.
- Sometimes creator may be owner too. In that case, it is similar to discretionary access control.
- The security access control is the combination of MAC and DAC.

Bell-LaPadula Model

- The Bell–LaPadula Model (BLP) is a state machine model used for enforcing access control in government and military applications.
- The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects.
- These security clearances are arranged in linear ordering and represent sensitivity levels. The security levels are *Top Secret*, *Secret*, *Confidential and Unclassified*.
- The higher the security clearance, the more sensitive the information (and the greater the need to keep it confidential).
- The State of state machine is used for the state transitions between these labels.

Bell-LaPadula Model

- The Bell–LaPadula model is built on the concept of a state machine with a set of allowable states in a computer system.
- The goal of Bell-LaPadula security model is to prevent access to objects at a security classification higher than the subject’s clearance.
- This model implements a combination of Mandatory Access Control and Discretionary Access Control, is primarily concerned with the confidentiality of the resource in question.

Bell-LaPadula Model

The Bell-LaPadula Model has <u>three basic properties</u>:

1. ***The simplest Security Property/No read-up***
   - It states that a subject at a given security level may not read an object at a higher security level. Subjects with a “Secret” clearance cannot access “Top Secret” objects, for example.
2. ***The *property / No write-down***

- It states that a subject at a given security level may not write (alter) to any object at a lower security level. For example, subjects who are logged into a Top Secret system cannot send emails to a secret system.

1. ***The Discretionary Security Property***
   - It states that if a subject has certain type of access on the object, he/she can transfer rights to other subject of their choice.

Bell-LaPadula Model

Strong Star Property

- The Strong Star Property is an alternative to the *-Property, in which subjects may write to objects with only a matching security level.
- Thus, the write-up operation permitted in the usual *-Property is not present, only a write-to-same operation.

Tranquility Principle

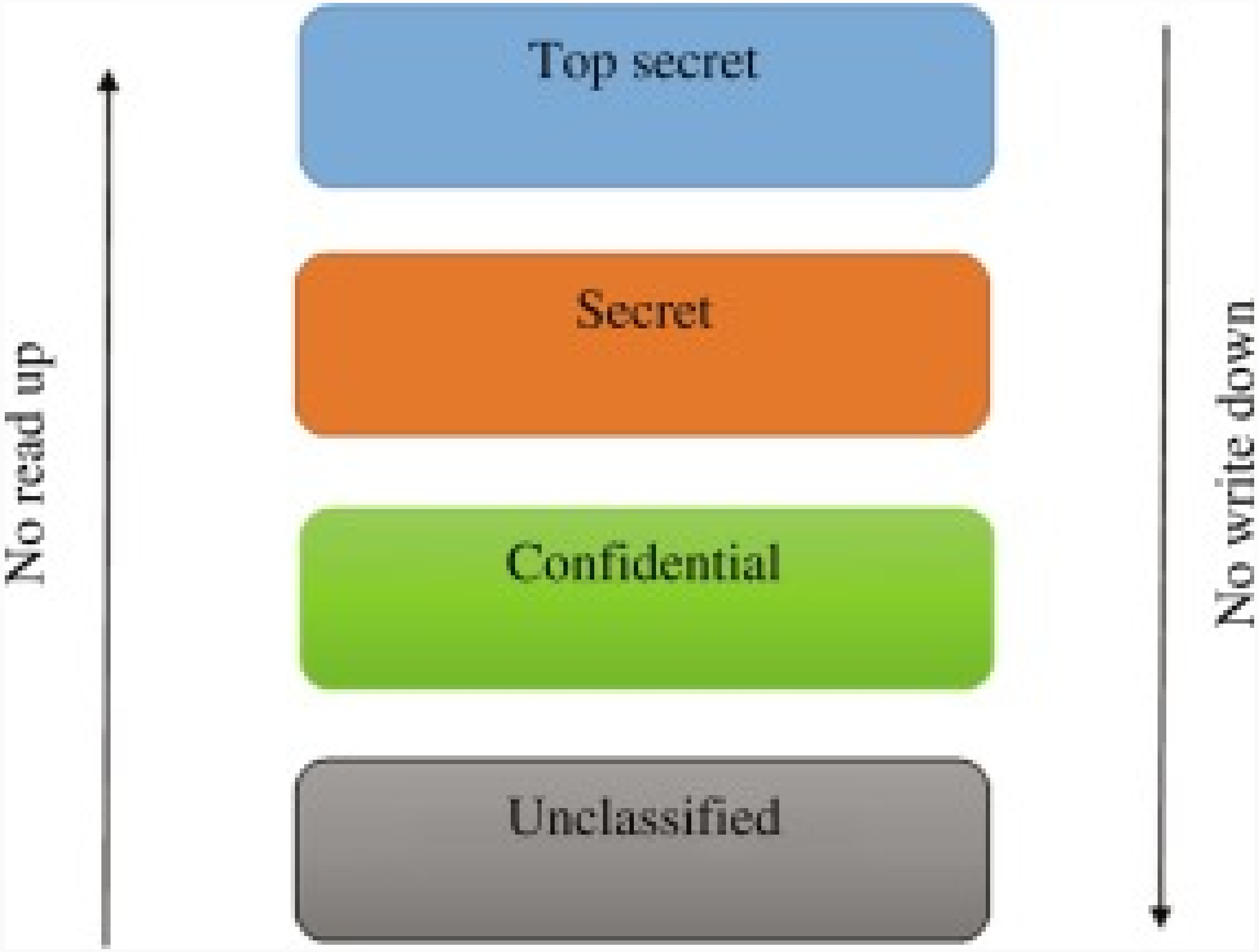
- The tranquility principle of the Bell–LaPadula model states that the classification of a subject or object does not change while it is being referenced.
- There are two forms to the tranquility principle: the "*principle of strong tranquility*" states that security levels do not change during the normal operation of the system. The "*principle of weak tranquility*" states that security levels may never change in such a way as to violate a defined security policy.

Bell-LaPadula Model

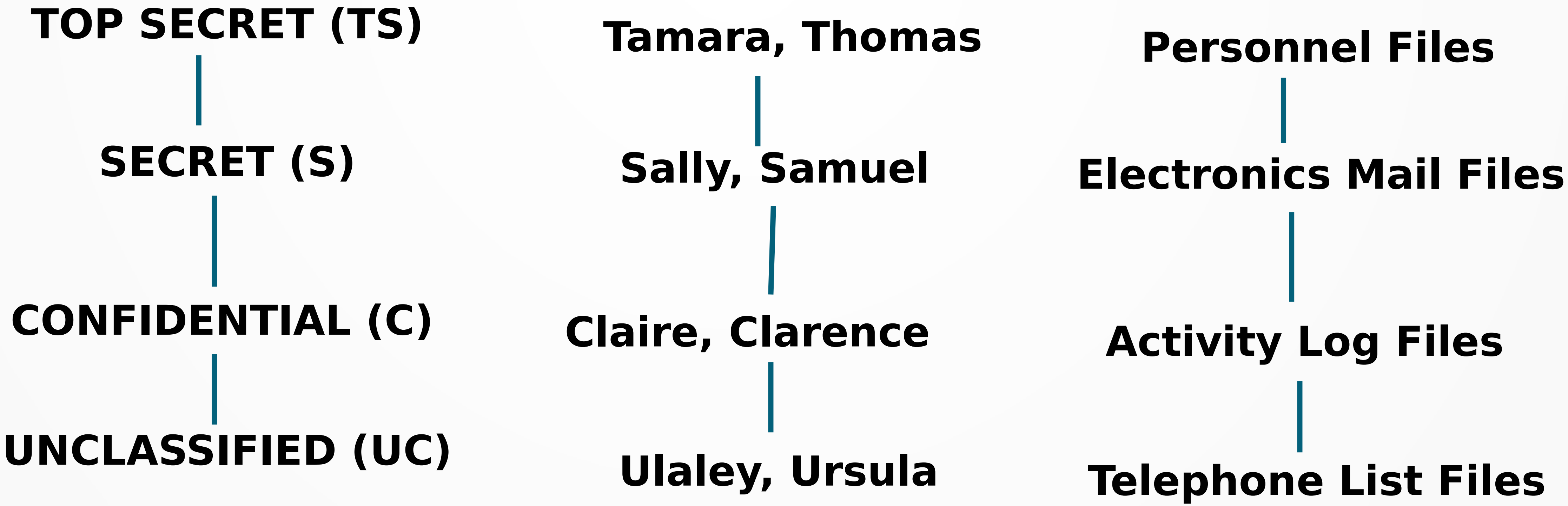
Limitations

- Only addresses confidentiality but limits integrity.
- The tranquility principle limits its applicability to systems where security levels do not change dynamically.

Bell-LaPadula Model



Example



TOP SECRET (TS)

SECRET (S)

CONFIDENTIAL (C)

UNCLASSIFIED (UC)

Tamara, Thomas

Sally, Samuel

Claire, Clarence

Ulaley, Ursula

Personnel Files

Electronics Mail Files

Activity Log Files

Telephone List Files

Fig: At the left is the basic confidentiality classification system. The four security levels are arranged with the most sensitive at the top and the least sensitive at the bottom. In the middle are individual grouped by their security clearances, and at the right is a set of documents grouped by their security levels.

Biba Integrity Model

- The *Biba Model* or *Biba Integrity Model* is a formal state transition system of data security policies designed to express a set of access control rules in order to ensure data integrity.
- Data and subjects are ordered by their levels of integrity into groups or arrangements.
- The levels of integrity are Untrusted, Slightly Trusted, Trusted, Highly Trusted, and Unimpeachable.

Biba Integrity Model

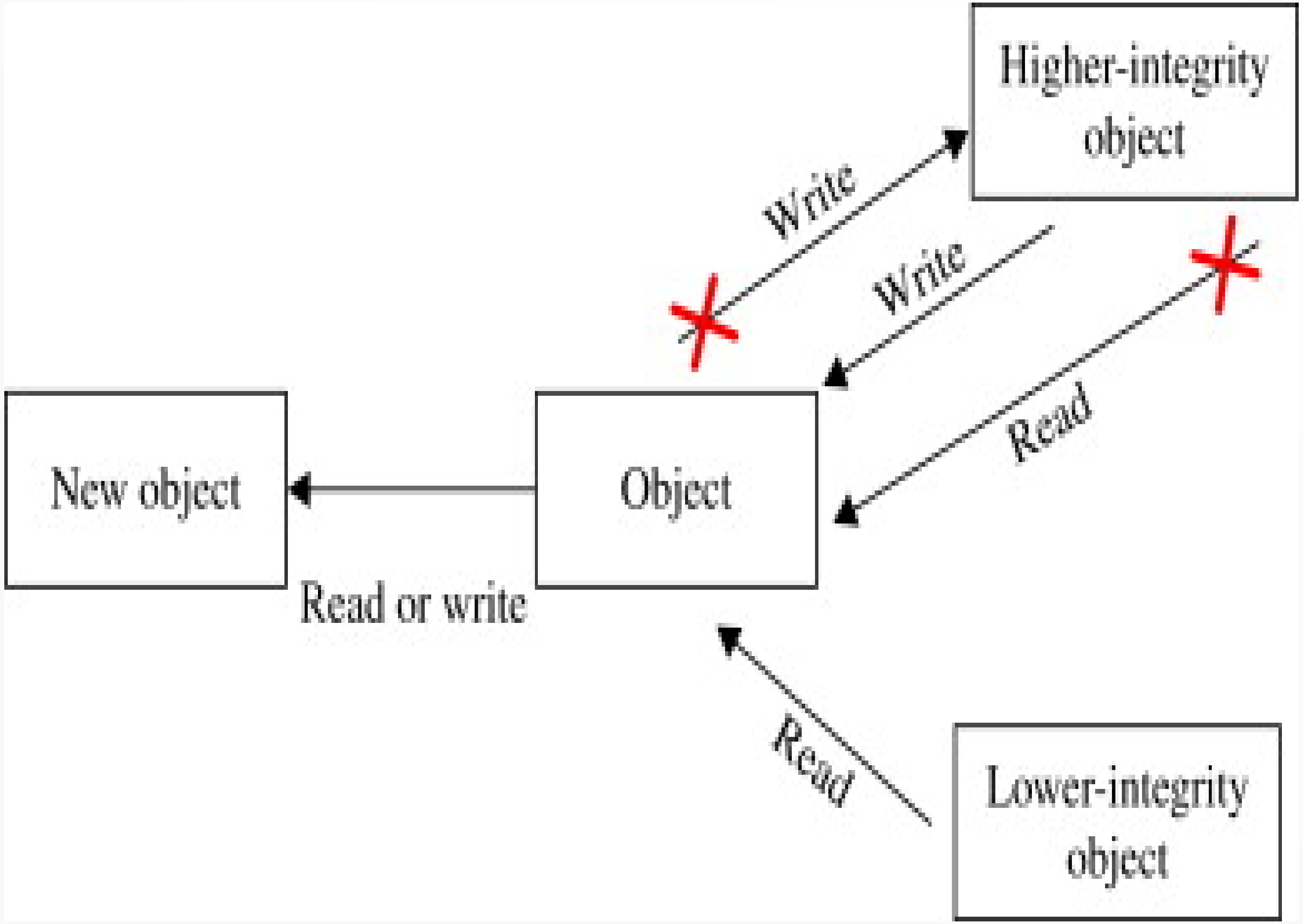
- Biba is designed so that a subject cannot corrupt data in a level ranked higher than the subject's and to restrict corruption of data at a lower level than the subject's.
- The Biba model was created to thwart a weakness in the Bell-LaPadula Model. The Bell-LaPadula model only addresses data confidentiality and not integrity.
- While many governments are primarily concerned with confidentiality, most businesses desire to ensure that the integrity of the information is protected at the highest level. *Biba* is the model of choice when integrity protection is vital.

Biba Integrity Model

The Biba model has two primary rules: the Simple Integrity Axiom and the * Integrity Axiom. (contrast to Bell-LaPadula Model)

- ***Simple Integrity Axiom***: “No read down”; a subject at a specific clearance level cannot read data at a lower classification. This prevents subjects from accessing information at a lower integrity level.
- **** Integrity Axiom***: “No write up”; a subject at a specific clearance level cannot write data to a higher classification. This prevents subjects from passing information up to a higher integrity level than they have clearance to change. This protects integrity by preventing bad information from moving up to higher integrity levels.

Biba Integrity Model



The model then defines a simple integrity policy that a subject may not read sources of lower integrity than his or her effective integrity rating, and a * property that a subject may only write objects that are of his or her effective integrity rating or lower.

Biba Integrity Model

- The Biba model is structurally similar to Bell-LaPadula but is intended to safeguard the integrity of information, rather than its confidentiality. The Biba model assigns integrity classifications to subjects and objects as an indication of reliability or trustworthiness. Subjects must have an integrity level equal to or lower than the objects they view, and cannot write information to an object at a higher integrity level. The Biba rules—sometimes simplified to “no read down” and “no write up”—guard against the corruption or loss of integrity of relatively more trusted information by preventing exposure to less trusted information.
- For transactional systems or technology-enabled business processes that place as much or more importance on protecting information integrity

Questions

- What do you mean by Access Control?
- Differentiate between security and safety?
- Differentiate between computer and network security?
- Why passive attacks are difficult to detect?
- Define active attacks with examples.
- State Biba Integrity Model.
- What are main goals of data integrity?
- List the categories of threat.
- What is disruption?
- What is Replay attack?

Questions

- Define access control. Explain the case of loss of integrity, loss of availability, loss of confidentiality with examples.