COMPUTER SECURITY AND CYBER LAW (CSCL)

LECTURER: ROLISHA STHAPIT/DIKSHYA SINGH

CONTENTS

CHAPTER 1

- **Unit 1: Introduction to computer security LH 5**
- Basic components of security (Confidentiality, Integrity and Availability), Security threats (Snooping, Modification, Masquerading, repudiation of origin, denial of receipt, Delay, Denial of service), Issues with security (Operational issues, human issues), Security Policies, Type of security policy, Access control, Type of access control (Introduction to MAC, DAC, Originator Controlled Access Control, Role Based Access Control) Overview of the Bell-LaPadula Model and Biba integrity model.
- **Assignment 1**

Why do we need security?

- Increased reliance on Information technology with or with out the use of networks
- The use of IT has changed our lives drastically.
- We depend on E-mail, Internet banking, and several other governmental activities that use IT
- Increased use of E-Commerce and the World Wide Web on the Internet as a vast repository of various kinds of information (immigration databases, flight tickets, stock markets etc.)

Need of security

- To safeguard the confidentiality, integrity, authenticity and availability of data transmitted over insecure networks
- Internet is not the only insecure network in this world
- Many internal networks in organizations are prone to insider attacks
- In fact, insider attacks are greater both in terms of likelihood of happening and damage caused

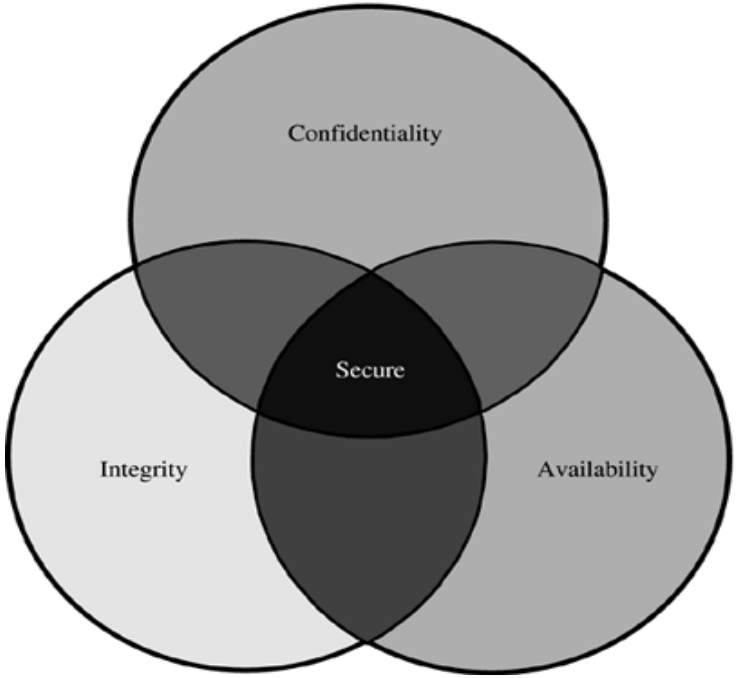
Some Security Terms

- **Computer Security:** Computer Security is the generic name for the collection of tools designed to protect data and to thwart hackers.
- **Network Security :** The network security is needed to protect data during their transmission
- **Internet Security:** Internet security measures to protect data during their transmission over a collection of interconnected networks. Internet security consists of measures to deter, prevent, detect, and correct security violations that involve the transmission and storage of information.

Computer Security / Information Security:

- Information security means protecting information and information systems from unauthorized access, use, modification, or destruction.
- The terms information security, computer security and information assurance are frequently used interchangeably.
- These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information.
- With the introduction of the computer, the need for automated tools for protecting the files and other information stored on the computer became evident. This is especially the case for a shared system as like internet.
- Thus, computer security is the generic name for the collection of tools designed to protect data and to prevent hackers.

Computer Security rests on confidentiality, integrity and availability (CIA)



Relationship between Confidentiality, Integrity and Availability

- **Confidentiality:** The confidentiality ensures that computer-related assets are accessed only by authorized party. That is, only those who should have access to something will actually get that access. Confidentiality is sometimes called secrecy or privacy. Confidentiality prevents unauthorized disclosure of data items.
- **Integrity:** The integrity means that assets can be modified only by authorized parties or only in authorized ways. Integrity prevents unauthorized modification. Modification includes writing, changing, deleting, creating.

- **Availability:** Availability means that assets are accessible to authorized parties at appropriate time. Availability prevents denial unauthorized access.

Availability is related to the capability of the information system being able to perform its intended tasks without any disruptions so that the data and information which need to be served by it are available as and when needed.

Apart from the above three pillars of security, other important aspects of security include

- Authenticity and
- Accountability.

- Authenticity ensures trustworthiness and genuineness of the information.
- Accountability relates to the capability of the information system to trace the activity of each entity to that particular entity. For example, if a person X does a certain change in a networked system, that system should have logs and audit trail facility to establish upon investigation that the change was actually done by X and not by other person.
- **Non-repudiation:**

Non repudiation prevents either sender or receiver from denying 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 received the message

Threats:

- A threat to a computing system is a set of circumstances that has the potential to cause loss or harm. It is a potential violation of security, means that it is a possible danger that might exploit vulnerability.
- **Attack** is an assault on system security that derives from an intelligent threat, i.e. attack is an intelligent act that is an intentional attempt to evade security services and violate the security policy of a system.
- Threats can be categorized into four classes:
- **Disclosure-** Unauthorized access to information

Eg: Snooping

- **Deception-** Acceptance of false data

Eg: Modification, Spoofing, denial of receipt, Repudiation of origin

- **Disruption-** Interruption of correct operation

Eg: Modification

- **Usurpation-** Unauthorized control of some part of system

Eg: Modification, Spoofing, denial of service, delay

Types of Security Threats

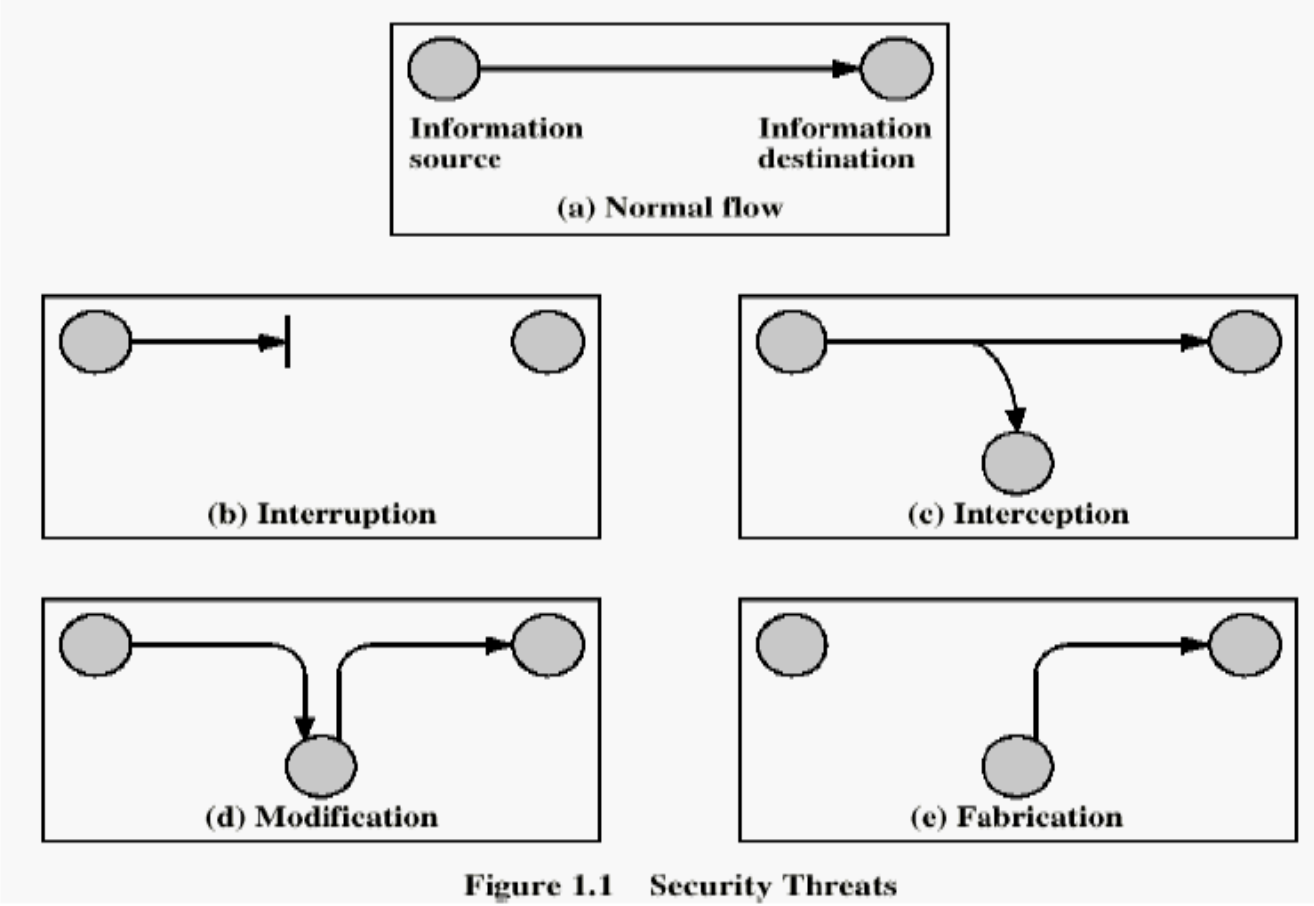


Figure 1.1 Security Threats

- **Interception:** An Interception means that some unauthorized party has gained access to an asset. The outside party can be a person, a program or a computing system. Example: The illicit copying the data files or programs
- **Interruption:** An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability. Example: the malicious destruction of a hardware device, malfunction of an operating system file manager, cutting of communication lines etc
- **Modification**: If an authorized party not only gains access to but tampers with an asset, this threat is called modification. Example, changing the values in data files, altering a program so that it performs differently. This is an attack on integrity.
- **Fabrication:** An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. Example: include insertion of spurious message in network.

Examples of Threat

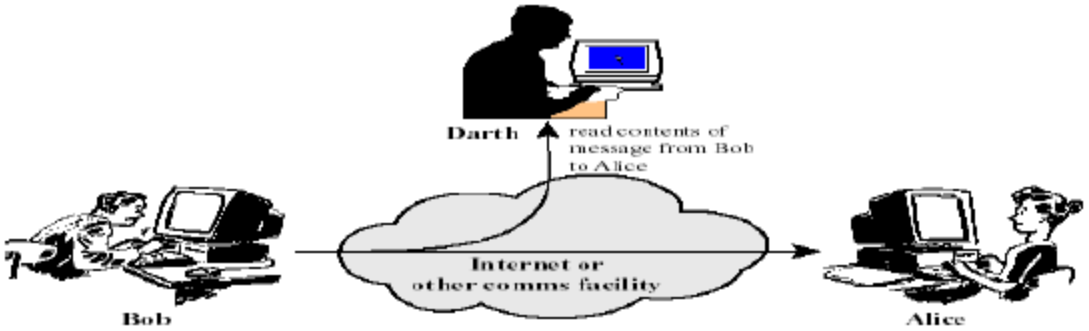
- **Snooping-** It is an unauthorized interception of information. It is passive, means that some entity is listening to communications or browsing the system information. Passive wiretapping is an example of snooping where attackers monitors the network communications.
- **Modification-** It is an unauthorized change of information. It is active, means that some entity is changing the information. Active wiretapping is an example of modification where data across the network is altered by the attackers.
- **Spoofing / Masquerading-** It is an imitation of one entity by another. E.g.: if a user tries to log into a computer across the internet but instead reaches another computer that claims to be the desired one, the user has been spoofed.

- **Repudiation of origin-** A false denial that an entity sent (or created) something, is a form of deception.
- **Denial of receipt-** A false denial that an entity received some message or information, is a form of deception.
- **Delay-** It is a temporal forbiddance of service. E.g.: If delivery of a message or a service requires time t; if an attacker can force the delivery time to be more than t, then there is delayed delivery.
- **Denial of service-** It is an infinite delay i.e., a long term inhibition of service. E.g., an entity may suppress all messages directed to a particular destination. 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 the performance.

Passive and active attacks

Passive attacks:

- No modification of content or fabrication
- Eavesdropping to learn contents or other information (transfer patterns, traffic flows etc.)



(a) Release of message contents

Active attacks:

- Modification of content and/or participation in communication to

❖ Impersonate legitimate parties

❖ Modify the content in transit

❖ Launch denial of service attacks

(a) Masquerade

Vulnerabilities

Vulnerability is a weakness in the security system. For example, in procedure, design, or implementation, there might be exploited to cause loss or harm. For instance, a particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user‘s identity before allowing data access.

- **Hardware Vulnerabilities:** Hardware is more visible than software. Interruption (Denial of services), interception (Theft), modification. Fabrication (substitution) constitutes the hardware vulnerabilities
- **Software Vulnerabilities:** Software can be replaced or destroyed maliciously, can be modified, deleted or misplaced accidentally, whether intentional or not these attacks exploit the software‘s vulnerabilities

Software deletion: software is surprisingly easy to delete

Software modification: Software is vulnerable to modification that either causes it to fail or causes it to perform an unintended task.

Software theft: A software theft performs unauthorized copying of software

Safeguards and Vulnerabilities

- A Safeguard is a countermeasure to protect against a threat
- A weakness in a safeguard is called vulnerability.

Policy and Mechanism

Security policy: A security policy is a statement of what is and what is not, allowed. That is the Policy says what is, and is not, allowed

- This defines —security for the site/system/etc.
- Policy definition: Informal? Formal?

Policy is a set of mechanisms by means of which your information security objectives can be defined and attained. Security policy governs a set of rules and objectives need by an organization.

The purpose of the information security policy is:

- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of data, applications, networks and computer systems.
- To define mechanisms that protect the reputation of the organization and allow the organization to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.
- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.

Protection State

- State is a collection of all possible values of the system.
- Subset of state that deals with protection is called Protection State.
- Current Protection State can be represented by using Access Control Matrix.
  - P be set of possible protection state.
  - Q be subset of P and it is set of state in which the system is authorized to reside.
  - P-Q is unsecure state.

Basic Properties of Security (Basic Principles of Security):

- **Confidentiality**: Let X be a set of entities and let I be some information. Then I has the property of confidentiality with respect to X if no member of X can obtain information about I. Confidentiality implies that information must not be disclosed to some set of entities. It may be disclosed to others. The membership of set X is often implicit – for example, when we speak of a document that is confidential. Some entity has access to the document. All entities not authorized to have such access make up the set X.
- **Integrity:** Let X be a set of entities and let I be some information or a resource. Then I has the property of integrity with respect to X if all members of X trust I. In addition to trusting the information itself, the members of X also trust that the conveyance and storage of I do not change the information or its trustworthiness (this aspect is sometimes called data integrity). If I is information about the origin of something, or about an identity, the members of X trust that the information is correct and unchanged (this aspect is sometimes called origin integrity or, more commonly, authentication). Also, I may be a resource rather than information. In that case, integrity means that the resource functions correctly (meeting its specifications). This aspect is called assurance. As with confidentiality, the membership of X is often implicit.

- **Availability**: Let X be a set of entities and let I be a resource. Then I has the property of availability with respect to X if all members of X can access I. The exact definition of "access" varies upon the needs of the members of X, the nature of the resource, and the use of the resource. If a book-selling server takes up to 1 hour to service a purchase request, that may meet the client's requirements for "availability." If a server of medical information takes up to 1 hour to service an anesthetic allergy information request, that will not meet an emergency room's requirements for "availability."

- **Security Mechanism:** A security mechanism is a tool or procedure for enforcing a security policy.
- Mechanisms may be

- Technical mechanism enforces the policy inside the system. For example, mechanism that enables a password to authenticate user before using the computer.

- Procedural mechanism enforces the policy outside the system. For example, mechanism that sensor's a disk containing a game program obtained from an unreliable source.

- Policies may be presented mathematically, as a list of allowed (secure) and disallowed (nonsecure) states. For our purposes, we will assume that any given policy provides an axiomatic description of secure states and nonsecure states. In practice, policies are rarely so precise; they normally describe in English what users and staff are allowed to do. The ambiguity inherent in such a description leads to states that are not classified as "allowed“ or"disallowed.

Goals of Security

- Given a security policy's specification of "secure" and "nonsecure" actions, these security mechanisms can prevent the attack, detect the attack, or recover from the attack. The strategies may be used together or separately.
- **Prevention**:

Prevention is to prevent the attackers from violating security policy. Prevention means that an attack will fail. Typically, prevention involves implementation of mechanisms that users can not override and that are trusted to be implemented in a correct ways so that the attacker can't defeat the mechanism by changing it.

- **Detection:**

It is most useful when an attack cannot be prevented, but it can also indicate the effectiveness of preventative measures. Detection mechanisms accept that an attack will occur; the goal is to determine that an attack is underway, or has occurred, and report it. The attack may be monitored, however, to provide data about its nature, severity, and results. Typical detection mechanisms monitor various aspects of the system, looking for actions or information indicating an attack.

- **Recovery:**

It has two forms. The first is to stop an attack and to assess and repair any damage caused by that attack.

In a second form of recovery, the system continues to function correctly while an attack is underway. This type of recovery is quite difficult to implement because of the complexity of computer systems.

For example if the attacker deletes a file, one recovery mechanism is to restore the file from backup tapes.

Assumptions and Trust

Security rests on assumptions specific to the type of security required and the environment in which it is to be employed. Eg: Opening a door requires a key , assumption is that the lock is secured against lock picking

Policy: A policy consists of set of axioms that the policy makers believe can be enforced. Designers of policies always makes two assumptions:

- First, the policy correctly and unambiguously partitions the set of system state into secure and unsecure states. The first assumption asserts that the policy is a correct description of what constitutes a secure system
- Second, Security mechanism prevents the system from entering an unsecure state. If either assumption is erroneous, the system will be unsecure. The second assumption says that the security policy can be enforced by security mechanism.

Trusting mechanisms requires several assumptions:

- Each mechanism is designed to implement one or more parts of the security policy.
- The union of the mechanism implements all aspects of the security policy
- The mechanisms are implemented correctly
- The mechanisms are installed and administrated correctly

Assurance

- Trust can not be quantified precisely. System specification, design and implementation can provide a basis for determining —how much? to trust a system. This aspect of trust is called **assurance.** It is an attempt to provide a basis for bolstering (specifying) how much one can trust a system.
- A system is said to satisfy a specification if the specification correctly states how the system will function.
- **Specification:** a specification is a (formal or informal) statement of the desired functioning of system.
- **Design:** The design of a system translates the specifications into components that will implement them.
- **Implementation:** The implementation creates a system that satisfies that design.
- A program is correct if its implementation performs as specified.

Issues with security

- Operational Issues
- Human Issues
- **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.

Cost-Benefit Analysis:

- Like any factor in a complex system, 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 because the data or resources can be reconstructed more cheaply than the protections themselves.
- Unfortunately, this is rarely the case.

- **Risk Analysis:**

➢ To determine whether an asset should be protected, and to what level, requires analysis of the potential threats against that asset and the likelihood that they will materialize.

➢ The level of protection is a function of the probability of an attack occurring and the effects of the attack should it succeed.

➢ First, risk is a function of environment.

➢ Second, the risks change with time.

➢ Third, many risks are quite remote but still exist.

➢ Finally, the problem of "analysis paralysis" refers to making risk analyses with no effort to act on those analyses.

- **Laws and Customs:**

  - Are desired security measures illegal?
  - Will people do them?

Human Issues:

- **Organizational Problems**

➢ Power and responsibility

➢ Financial benefits

- **People problems:**

➢ Heart of any security system is people. This is particularly true in computer security.

➢ Outsiders: Peoples who have some motive to attack an organization and are not authorized to use that organization‘s systems are called Outsiders and can pose a serious threat..

➢ Insiders: Insiders are those employees who are authorized to use the system and misuse the authorized privilege.

Security Policies

- A security policy defines "secure" for a system or a set of systems.
- Security policies can be informal or highly mathematical in nature.
- Consider a computer system to be a finite-state automaton with a set of transition functions that change state.
- Then: A security policy is a statement that partitions the states of the system into a set of authorized, or secure, states and a set of unauthorized, or nonsecure, states.
- A security policy sets the context in which we can define a secure system. What is secure under one policy may not be secure under a different policy.

Types of Security Policies

- Each site has its own requirements for the levels of confidentiality, integrity, and availability, and the site policy states these needs for that particular site.
- A ***military security policy (also called a governmental security policy)*** is a security policy developed primarily to provide confidentiality.
- A ***commercial security policy*** is a security policy developed primarily to provide integrity.
- A ***confidentiality policy*** is a security policy dealing only with confidentiality.
- An ***integrity policy*** is a security policy dealing only with integrity.
- 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. A similar distinction holds for integrity policies and commercial policies.

Access Control

- It is an ability to permit or deny the use of a particular resource by a particular entity.
- Subject: Entity that perform action
- Object: Entity representing resource

Access Control Matrix:

- **Protection state of system**

  - Describes current settings, values of system relevant to protection

- **Access control matrix**

  - Access control matrix is one tool that describes current protection state precisely

  - Matrix describing rights of subjects

  - State transitions change elements of matrix

- The simplest framework for describing a protection system is the access control matrix model, which describes the rights of users over files in a matrix
- UNIX defines read, write, execute, append and own for accessing the fie by the processes presenting resource

Types of Access Control

- A security policy may use two types of access controls, alone or in combination.
- In one, access control is left to the discretion of the owner.
- In the other, the operating system controls access, and the owner cannot override the controls.

1. **Discretionary Access Control (DAC) or Identity Based Access Control (IBAC):**

- Individual user sets access control mechanism to allow or deny access to an object.
- Discretionary access controls base access rights on the identity of the subject and the identity of the object involved.
- Identity is the key; the owner of the object constrains who can access it by allowing only particular subjects to have access.
- The owner states the constraint in terms of the identity of the subject, or the owner of the subject

2. Mandatory Access Control (MAC) or Rule Based Access Control:

- System mechanism controls access to object, and individual cannot alter that access based on rule.
- The operating system enforces mandatory access controls.
- Neither the subject nor the owner of the object can determine whether access is granted.
- Typically, the system mechanism will check information associated with both the subject and the object to determine whether the subject should access the object.
- Rules describe the conditions under which access is allowed.

3. Originator Access Control (ORCON or ORGCON):

- Controlled by originator (creator) of information controls who can access information.
- 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.
- The owner of the file has no control over who may access the file.

4. Role Based Access Control:

- The ability, or need, to access information may depend on one's job functions
- A role is a collection of job functions
- is an approach to restricting system access to authorized users

Security Models

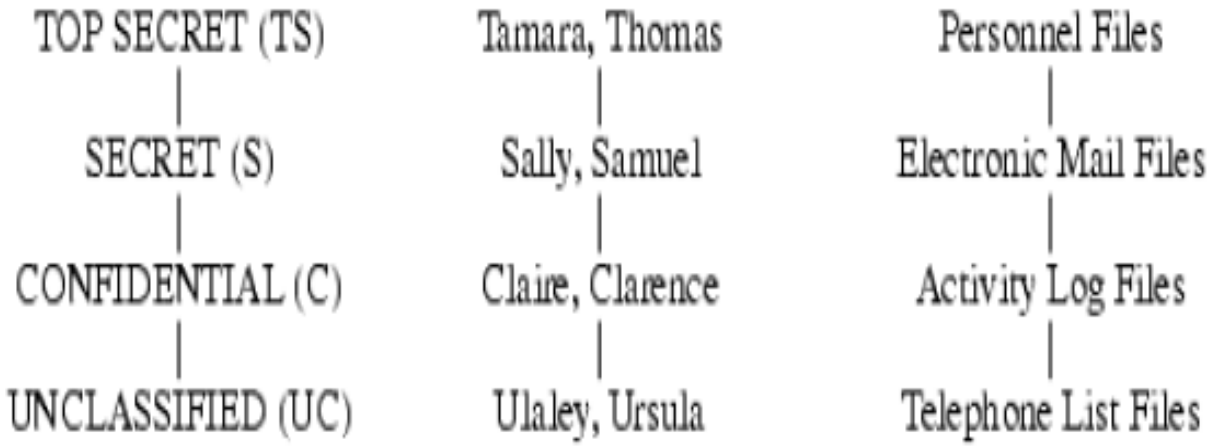
- A security policy governs a set of rules and objectives need by an organization.
- A security model can be used by an organization to help express the policy or business rules to be used in a computer system.

The Bell-LaPadula Model

- It is based on Confidentiality Policy
- The Bell-LaPadula model is one of the first models that was created to control access to data.
- The properties of the Bell-LaPadula model are:
  - The simple security property which is —no read up
  - The star property which is —no write down.
- A problem with this model is it does not deal with the integrity of data.
- The Bell-LaPadula Model corresponds to military-style classifications.

- A confidentiality policy, also called an *information flow policy*, prevents the unauthorized disclosure of information.
- Unauthorized alteration of information is secondary.
- The simplest type of confidentiality classification is a set of *security clearances* arranged in a linear (total) ordering.
- These clearances represent sensitivity levels.
- The higher the security clearance, the more sensitive the information (and the greater the need to keep it confidential).
- A subject has a *security clearance*.

Figure 5-1. 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 individuals grouped by their security clearances, and at the right is a set of documents grouped by their security levels.



- In the figure, Claire's security clearance is C (for CONFIDENTIAL), and Thomas' is TS (for TOP SECRET). An object has a security classification; the security classification of the electronic mail files is S (for SECRET), and that of the telephone list files is UC (for UNCLASSIFIED).
- The goal of the Bell-LaPadula security model is to prevent read access to objects at a security classification higher than the subject's clearance.

Biba Integrity Model

- In 1977, Biba studied the nature of the integrity of systems.
- The Biba security model was developed to address a weakness in the Bell-La Padula model.
- The Biba model addresses integrity which was missing in the confidentiality focused Bell-La Padula model.
- Much like the Bell-La Padula model, the Biba model uses objects and subjects.
- However, objects and subjects are grouped into integrity levels instead of given security labels.
- The Biba Model also carries a clever catch phrase: **—no read down, no write up.**

- In order to preserve integrity, subjects may create content at or below their own integrity level and view content at or above their own integrity level.
- This helps to prevent data corruption thus preserving integrity. In similar fashion to the Bell-La Padula model, the Biba model also has a couple of security rules:

- A subject at a given level of integrity must not read an object at a lower integrity level (no read down). This is known as the Simple Integrity Axiom.

- A subject at a given level of integrity must not write to any object at a higher level of integrity (no write up). This is known as the * (star) Integrity Axiom.

THE END

Chapter 1 Test
Coming Soon

STUDY TONIGHT!