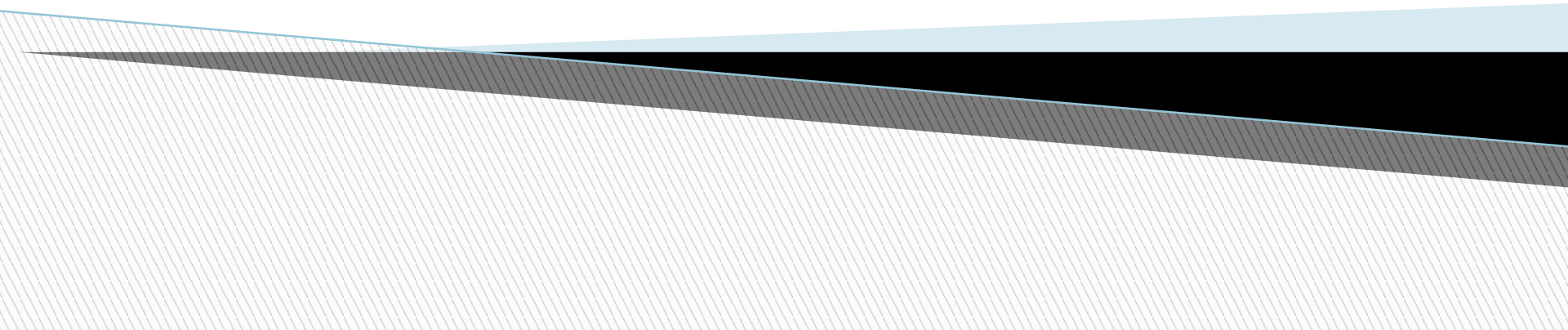
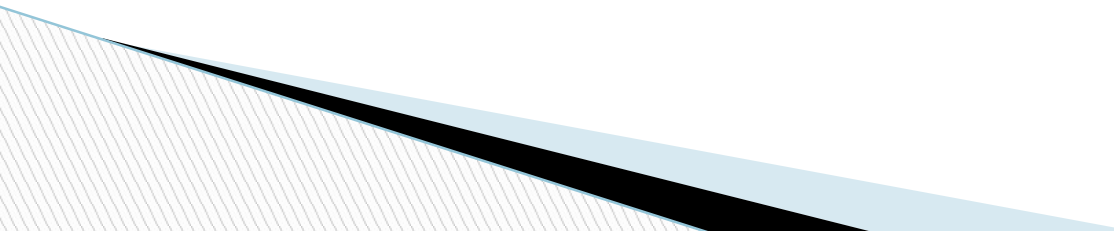


CYBER SECURITY

BY- SAMIKSHA BISHT



CONTENT

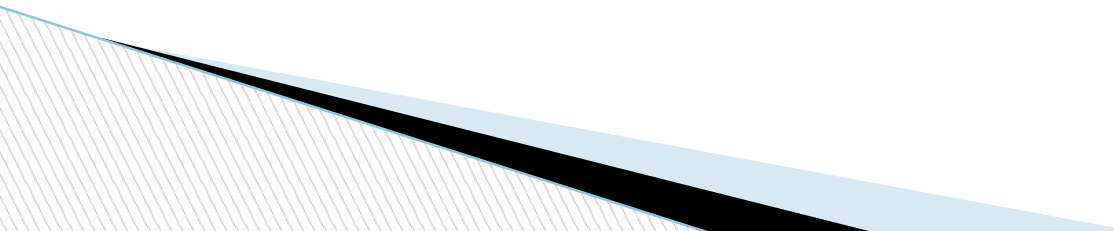
- Principles of cyber security
 - Interrelated components of the computing environment .
 - Cyber security models.
 - Need for cyber security models .
- 

Principles of cyber security

- There are three principles of cyber security they are **confidentiality, integrity, and availability**.
- Together it is also known as CIA triad.

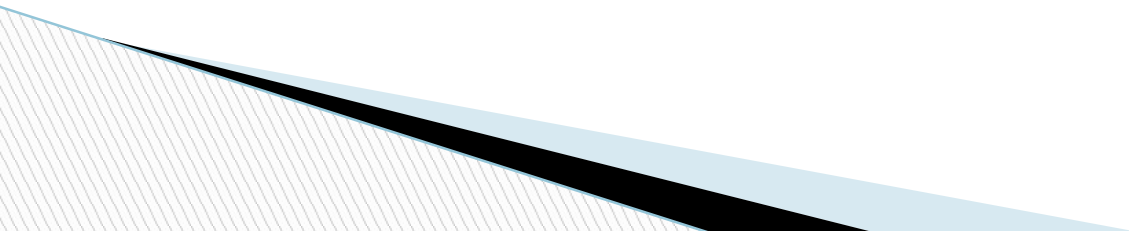
CIA Explanation

- What is Confidentiality?
 - **Confidentiality** measures are designed to protect against unauthorized disclosure of information. The objective of the confidentiality principle is to ensure that private information remains private and that it can only be viewed or accessed by individuals who need that information in order to complete their job duties.

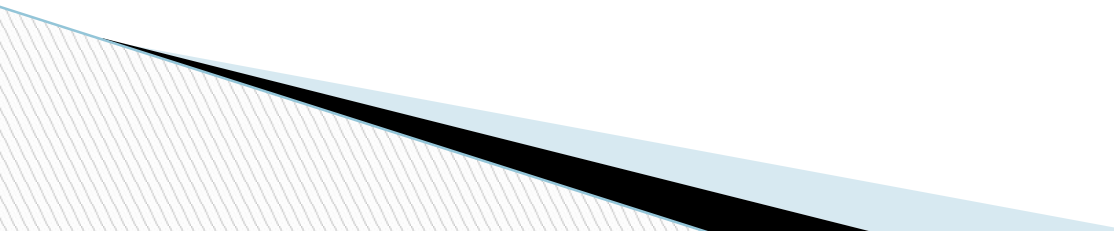
 - What is Integrity?
 - **Integrity** involves protection from unauthorized modifications (e.g., add, delete, or change) of data. The principle of integrity is designed to ensure that data can be trusted to be accurate and that it has not been inappropriately modified.
 -
 - What is Availability?
 - **Availability** is protecting the functionality of support systems and ensuring data is fully available at the point in time (or period requirements) when it is needed by its users. The objective of availability is to ensure that data is available to be used when it is needed to make decisions.
- 

What is Computing environment

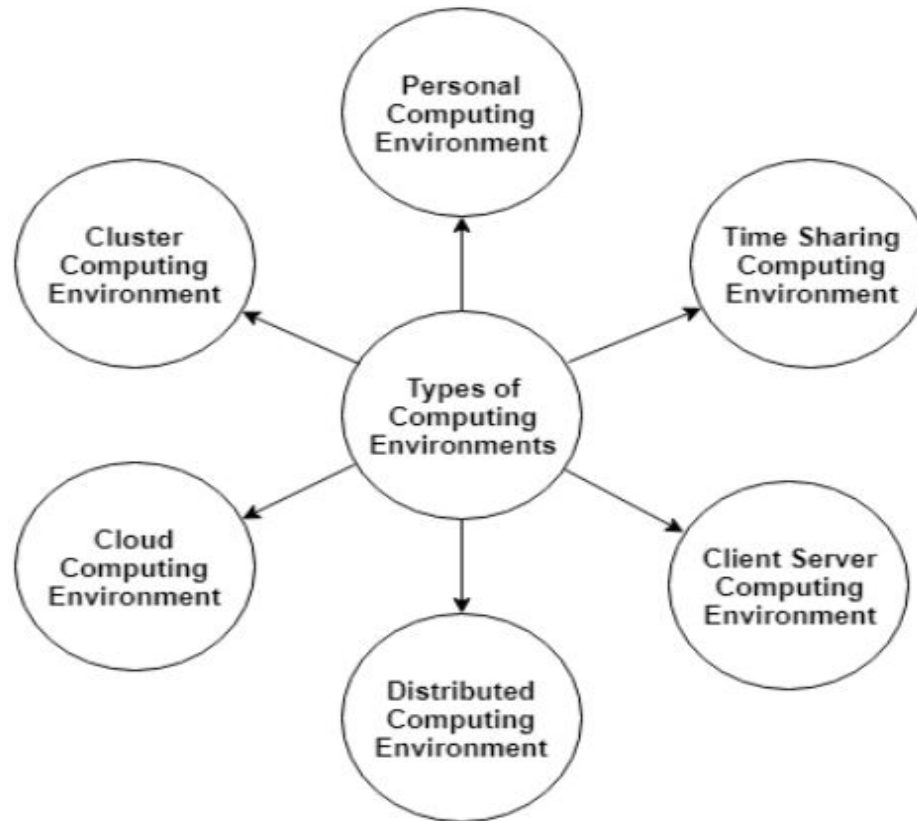
- Environment where many computers are interlinked and are capable of handling multiple issues along with exchange of information .



Computing Environment

- In the study, Computing Environment is defined as a structured environment, which encompasses software and hardware and provides computer services, support and maintenance. This includes networking, application and security infrastructures. Computing has long been a significant element in the operation of many organizations that deploy it.
 - With this increasing role, investment in computing systems and technologies, assets and support have become a significant element in the organizations that it supports.
- 

Types of computing environment

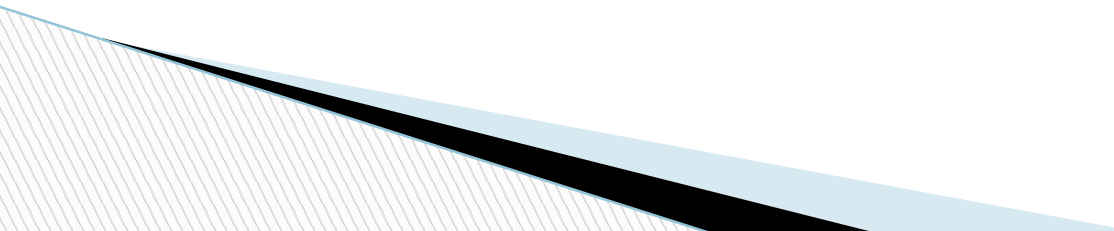


Cyber Security Models

- A **computer security model** is a scheme for specifying and enforcing security policies. A security model may be founded upon a formal model of access rights, a model of computation, a model of distributed computing, or no particular theoretical grounding at all. A computer security model is implemented through a computer security policy.

Purpose of cyber security model

The main purpose of cyber security model is to answer the following questions .

- □ How a network or system design change might help or hurt (performance, security, usability) ?
 - □ How well a network can withstand or protect against an attack ?
 - □ Whether a new product will make a set of systems “more secure” ?
 - □ What an optimal deployment or design of a system change might be?
- 

Different types of security models

□ **State Machine Model**

- The *state machine model* is based on a finite state machine, as shown in Figure 5.6. State machines are used to model complex systems and deals with acceptors, recognizers, state variables, and transaction functions. The state machine defines the behavior of a finite number of states, the transitions between those states, and actions that can occur.

□ **Information Flow Model**

- The *Information Flow model* is an extension of the state machine concept and serves as the basis of design for both the Biba and Bell-LaPadula models, which are discussed in the sections that follow. The Information Flow model consists of objects, state transitions, and lattice (flow policy) states. The real goal of the information flow model is to prevent unauthorized, insecure information flow in any direction. This model and others can make use of guards. Guards allow the exchange of data between various systems.

□



Contd.

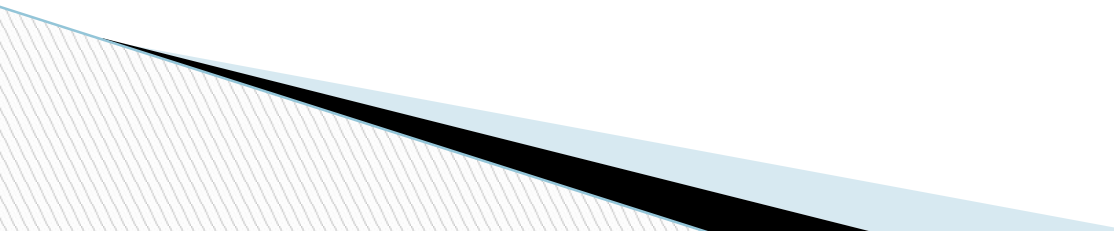
❑ **Noninterference Model**

- ❑ The *Noninterference* model as defined by Goguen and Meseguer was designed to make sure that objects and subjects of different levels don't interfere with the objects and subjects of other levels. The model uses inputs and outputs of either low or high sensitivity. Each data access attempt is independent of all others and data cannot cross security boundaries.

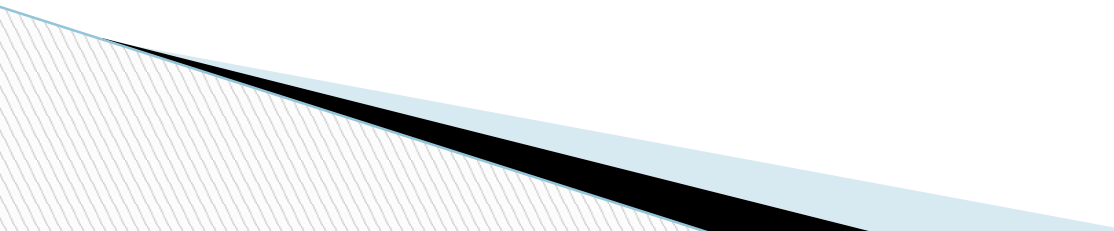
❑ **Bell-LaPadula**

- ❑ The *Bell-LaPadula* state machine model enforces confidentiality. The Bell-LaPadula model uses mandatory access control to enforce the DoD multilevel security policy. For a subject to access information, he must have a clear need to know and meet or exceed the information's classification level.

Contd.

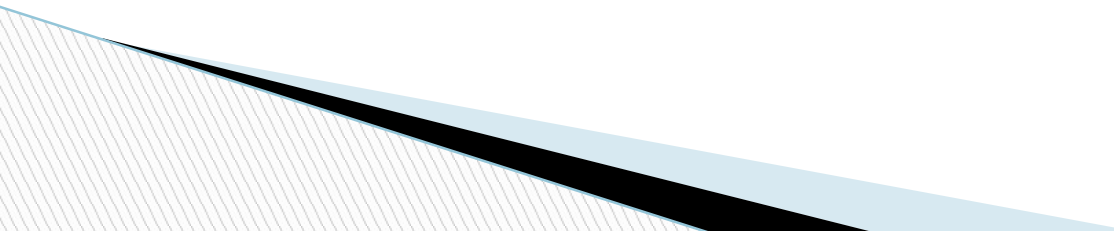
- ❑ The Bell-LaPadula model is defined by the following properties:
 - ❑ **Simple security property (ss property)**—This property states that a subject at one level of confidentiality is not allowed to read information at a higher level of confidentiality. This is sometimes referred to as “no read up.”
 - ❑ **Star * security property**—This property states that a subject at one level of confidentiality is not allowed to write information to a lower level of confidentiality. This is also known as “no write down.”
 - ❑ **Strong star * property**—This property states that a subject cannot read/write to object of higher/lower sensitivity.
- 

Contd.

- The *Biba model* was the first model developed to address the concerns of integrity. Originally published in 1977, this lattice-based model has the following defining properties:
 - **Simple integrity property**—This property states that a subject at one level of integrity is not permitted to read an object of lower integrity.
 - **Star * integrity property**—This property states that an object at one level of integrity is not permitted to write to an object of higher integrity.
 - **Invocation property**—This property prohibits a subject at one level of integrity from invoking a subject at a higher level of integrity.
- 

Contd.

□ **Clark-Wilson**

- The *Clark-Wilson* model was created in 1987. It differs from previous models because it was developed with the intention to be used for commercial activities. This model addresses all the goals of integrity. Clark Wilson dictates that the separation of duties must be enforced, subjects must access data through an application, and auditing is required. Some terms associated with Clark Wilson include
 - User
 - Transformation procedure
 - Unconstrained data item
 - Constrained data item
 - Integrity verification procedure
- 

Contd.

❑ **Take-Grant Model**

- ❑ The *Take-Grant* model is another confidentiality-based model that supports four basic operations: take, grant, create, and revoke. This model allows subjects with the take right to remove take rights from other subjects. Subjects possessing the grant right can grant this right to other subjects. The create and revoke operations work in the same manner: Someone with the create right can give the create right to others and those with the revoke right can remove that right from others.

❑ **Brewer and Nash Model**

- ❑ The *Brewer and Nash* model is similar to the Bell-LaPadula model and is also called the *Chinese Wall model*. It was developed to prevent conflict of interest (COI) problems. As an example, imagine that your security firm does security work for many large firms. If one of your employees could access information about all the firms that your company has worked for, he might be able to use this data in an unauthorized way. Therefore, the Chinese Wall model is more context oriented in that it prevents a worker consulting for one firm from accessing data belonging to another, thereby preventing any COI.

Other models

- A security model defines and describes what protection mechanisms are to be used and what these controls are designed to achieve. Although the previous section covered some of the more heavily tested models, you should have a basic understanding of a few more. These security models include
 - **Graham Denning model**—This model uses a formal set of protection rules for which each object has an owner and a controller.
 - **Harrison-Ruzzo-Ullman model**—This model details how subjects and objects can be created, deleted, accessed, or changed.
 - **Lattice model**—This model is associated with MAC. Controls are applied to objects and the model uses security levels that are represented by a lattice structure. This structure governs information flow. Subjects of the lattice model are allowed to access an object only if the security level of the subject is equal to or greater than that of the object. Every subset has a least upper bound and a greatest lower bound.
- 