Protection Models

Information Security

Arfan Shahzad
{ arfanskp@gmail.com }

Course Outline

Course Name: Information Security
Credit Hours: 3(3-0)
Prerequisites: Data Communication and Computer Networks
Course Outline:
Basic notions of confidentiality, integrity, availability; authentication models; protection models; security kernels; Encryption, Hashing and Digital Signatures; audit; intrusion detection and response; database security, hostbased and network-based security issues operational security issues; physical security issues; personnel security; policy formation and enforcement; access controls; information flow; legal and social issues; identification and authentication in local and distributed systems; classification and trust modeling; risk assessment
Reference Materials:
1. *Computer Security: Art and Science*, Matthew Bishop
2. *Cryptography and Network Security* by William Stalling 6th Edition, 2012
3. *Principles of Information Security* 3rd E by Michael E. Whitman and Herbert J. Mattord

Protection Models

- In information security, protection models refer to the ***various methods and techniques*** **used to protect systems and data** ***from unauthorized access***, ***use***, ***disclosure***, ***disruption***, ***modification***, or ***destruction***.
- Here are some common protection models:

Protection Models cont…

1. Access Control Model
2. Confidentiality Model
3. Integrity Model
4. Availability Model
5. Defense in Depth Model
6. Least Privilege Model
7. Principle of Least Astonishment (POLA) Model

Protection Models cont…
Access Control Model

- The Access Control Model is a **security model** that **governs** ***how users are granted access*** to system resources and data.
- It determines the **mechanisms** and **rules** for ***authentication***, ***authorization***, and ***accounting*** (AAA) in order to ***enforce proper access controls***.
- The goal of the Access Control Model is to ensure that ***only authorized individuals or processes*** **are allowed** ***to access specific resources*** or ***perform certain actions*** within a system.

Protection Models cont…
Access Control Model

- There are several types of Access Control Models, including:

1. Mandatory Access Control (MAC)
2. Discretionary Access Control (DAC)
3. Role-Based Access Control (RBAC)
4. Attribute-Based Access Control (ABAC)
5. Rule-Based Access Control (RBAC)

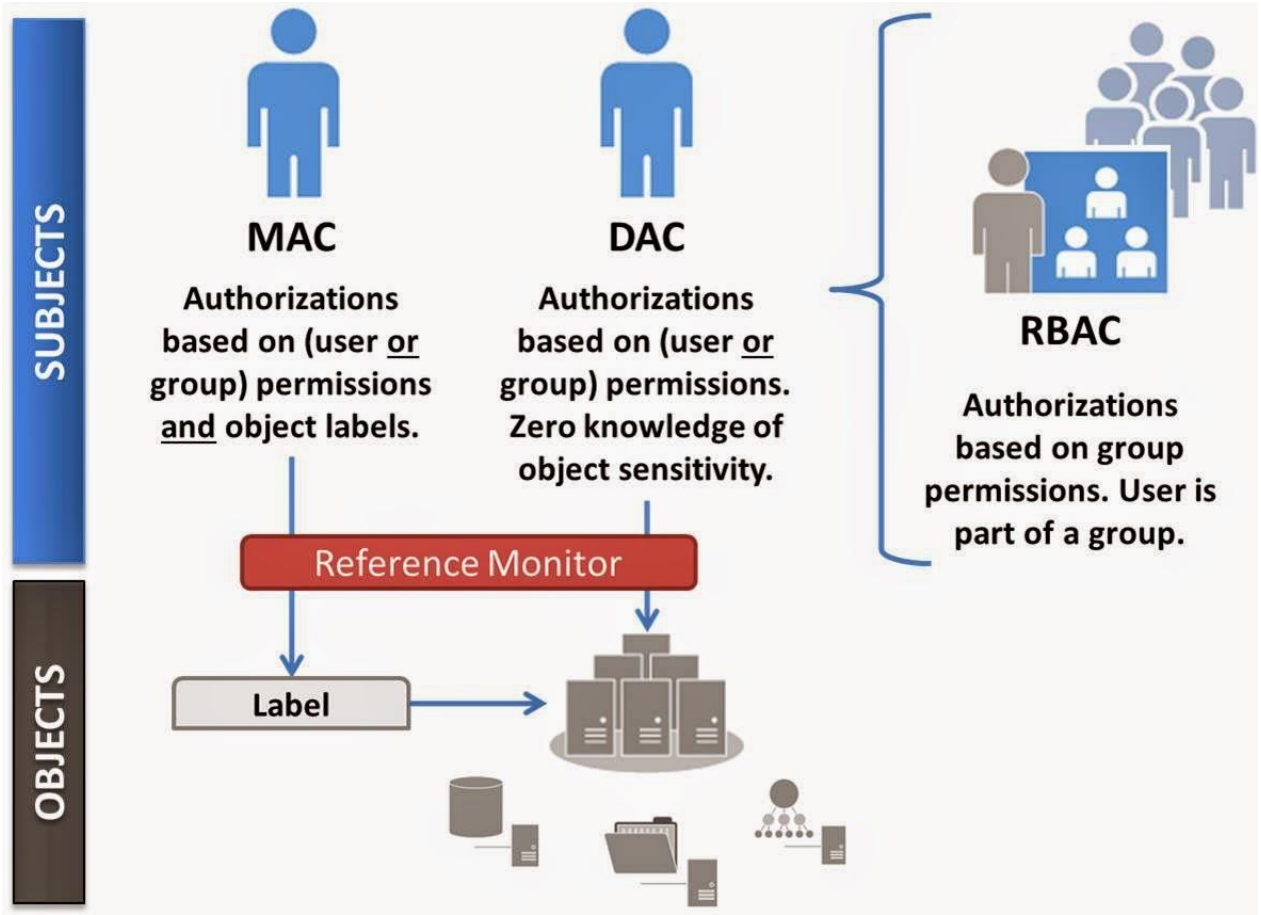
Protection Models cont…

Access Control Model: Mandatory Access Control (MAC)

- This model assigns **security labels** (e.g., security classifications or levels) to both ***users*** and ***system resources***.
- Access decisions are based on the ***labels*** and predefined ***access rules***, which are typically enforced by the **operating system** or **security software**.

Protection Models cont…

Access Control Model: Mandatory Access Control (MAC)



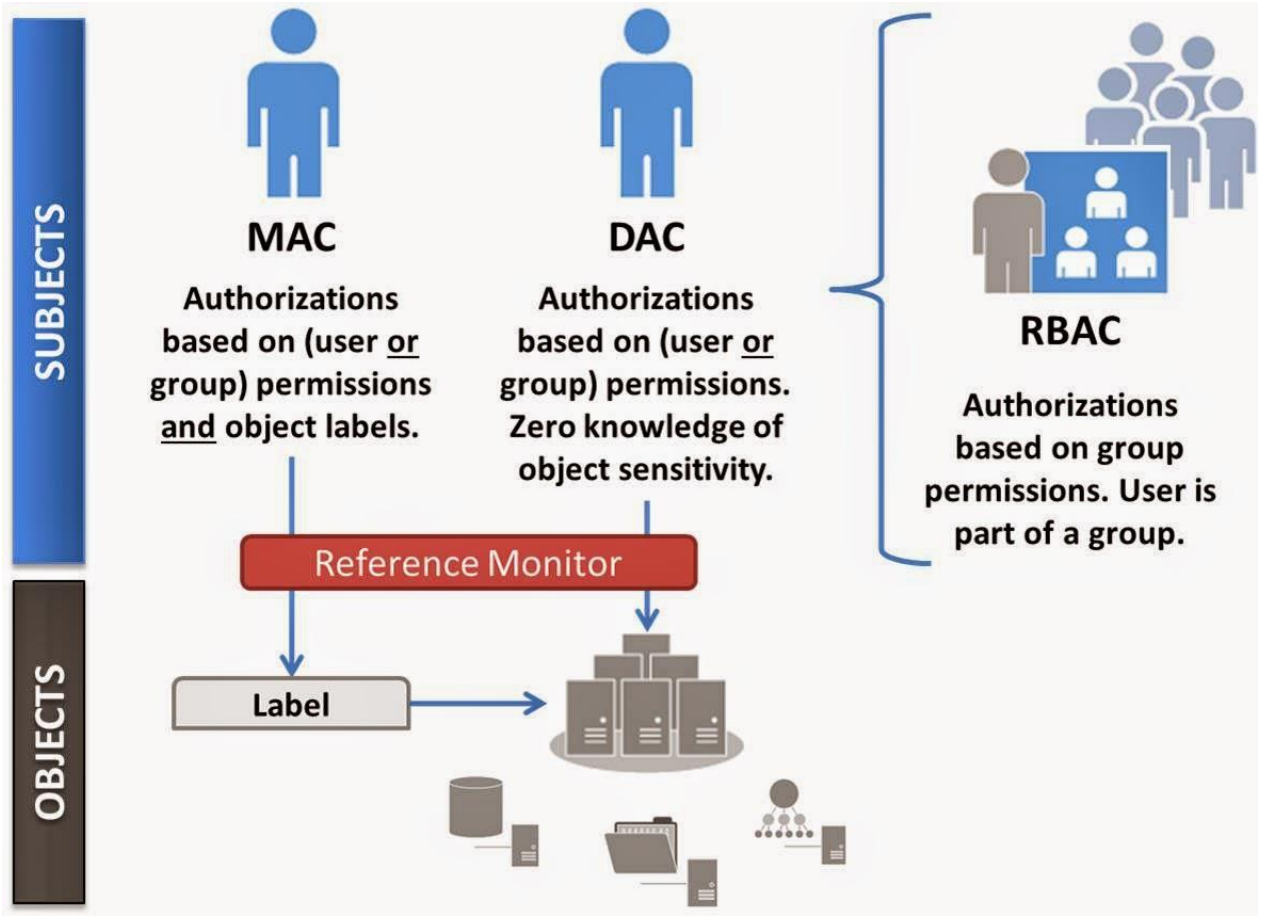
Protection Models cont…

Access Control Model: Discretionary Access Control (DAC)

- In this model, access control decisions are left to the ***discretion*** of the **resource owner**.
- Each resource has an associated **Access Control List** (ACL) that ***specifies the permissions granted*** to **individual users** or **groups**.

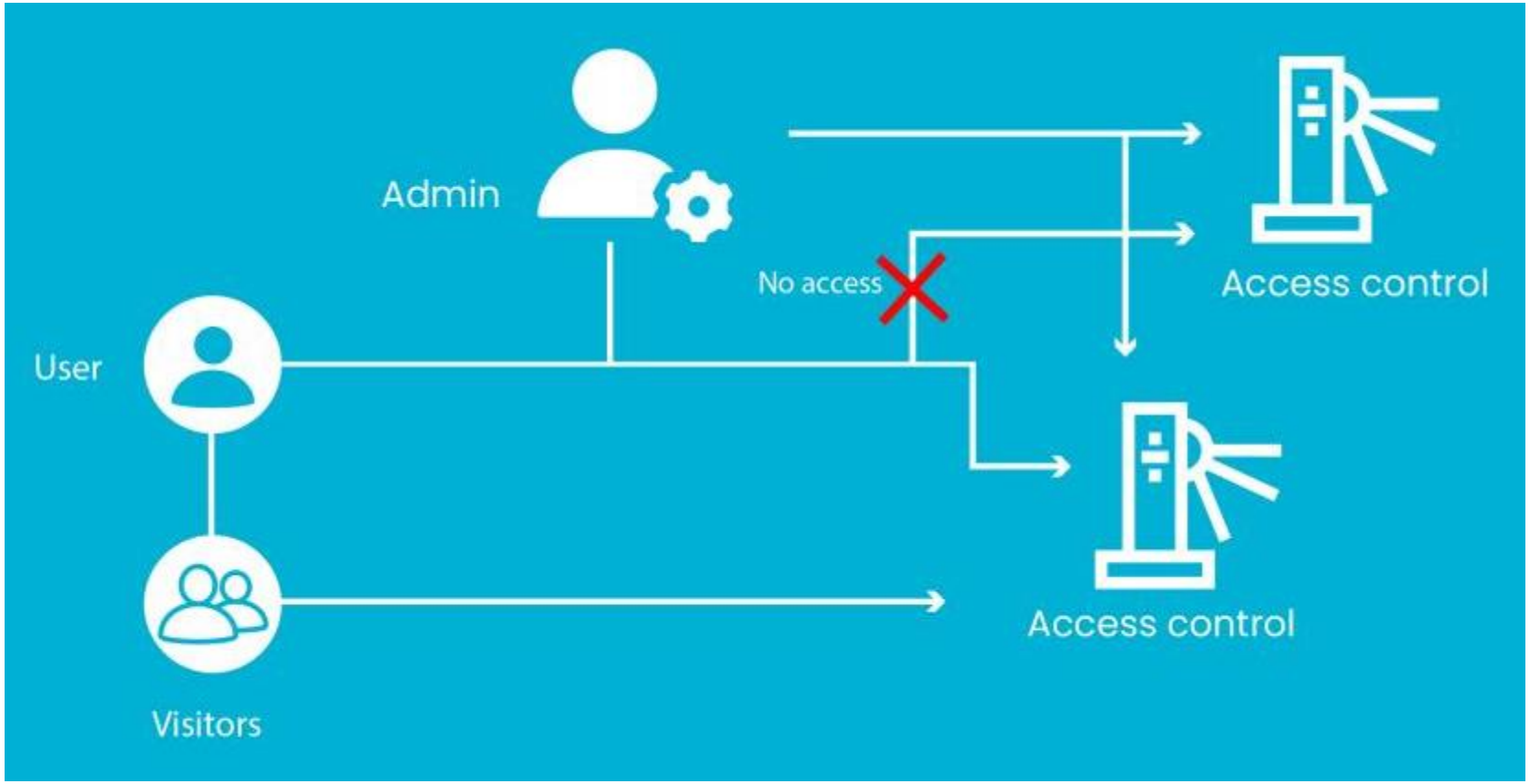
Protection Models cont…

Access Control Model: Discretionary Access Control (DAC)



Protection Models cont…

Access Control Model: Discretionary Access Control (DAC)



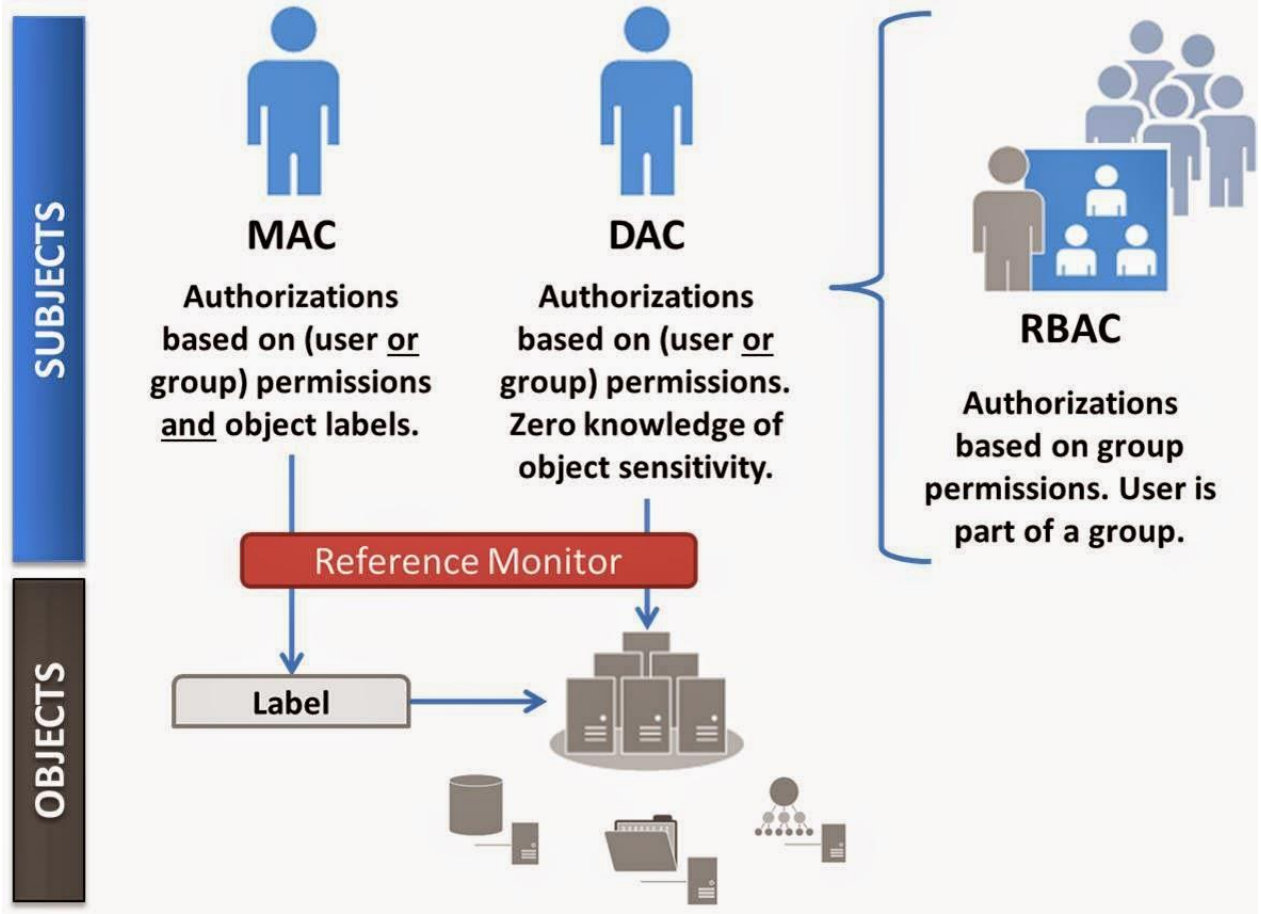
Protection Models cont…

Access Control Model: Role-Based Access Control (RBAC)

- RBAC is based on the concept of **roles**.
- Users are assigned specific ***roles***, and ***permissions are assigned*** to these ***roles*** rather than to ***individual users***.
- This simplifies administration and enables more efficient management of access controls.

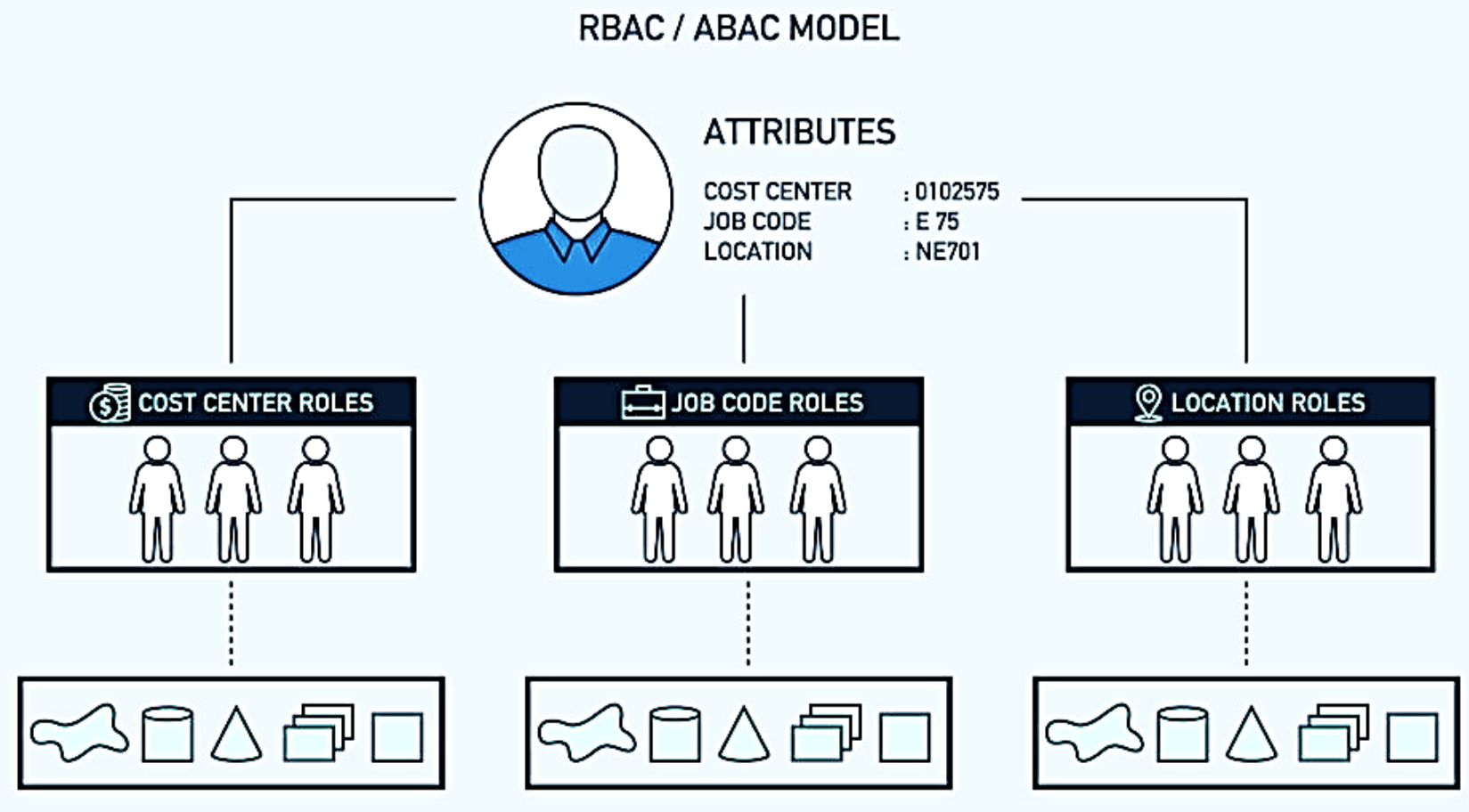
Protection Models cont…

Access Control Model: Role-Based Access Control (RBAC)



Protection Models cont…

Access Control Model: Role-Based Access Control (RBAC)



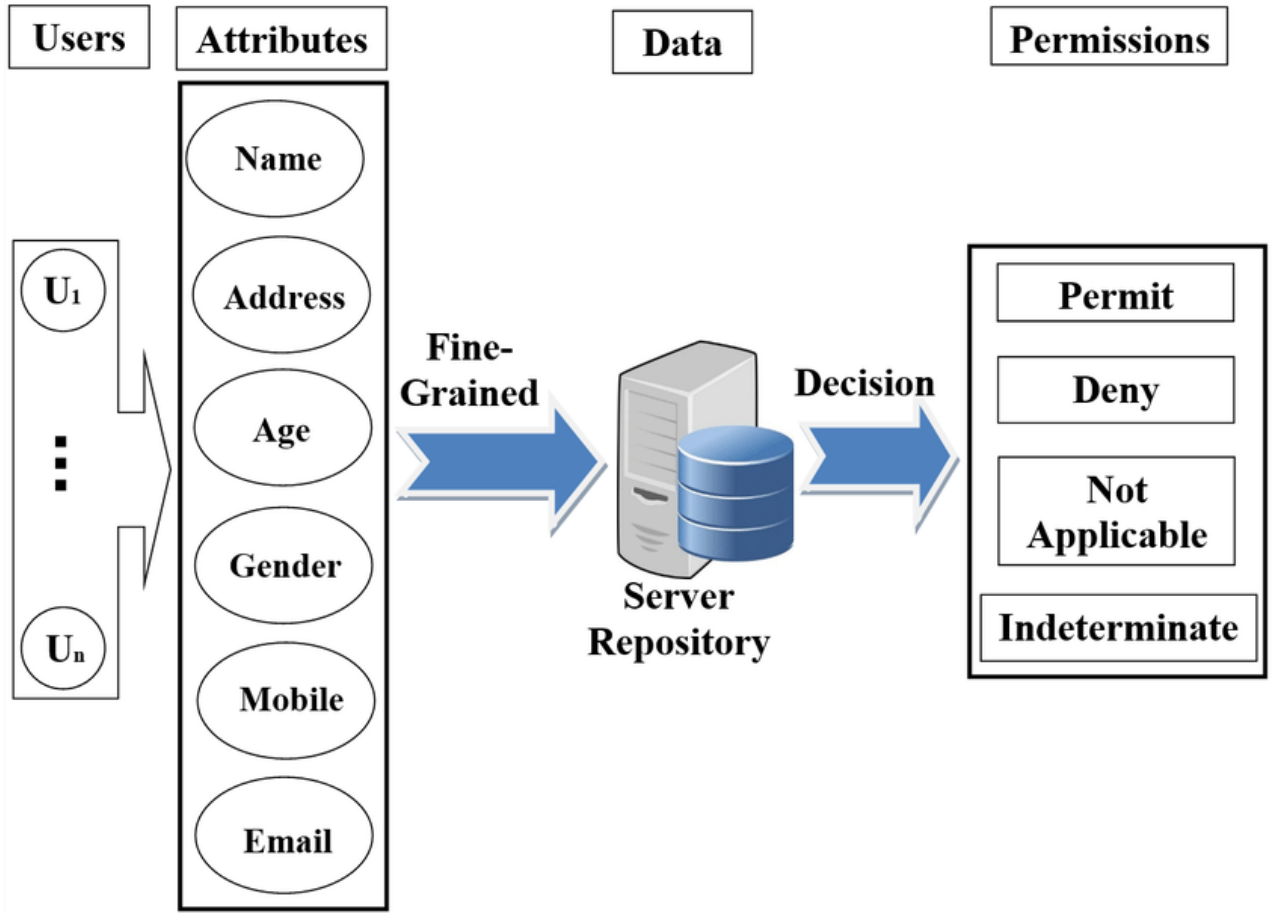
Protection Models cont…

Access Control Model: Attribute-Based Access Control (ABAC)

- ABAC takes into account ***various attributes*** or ***characteristics*** of **users**, **resources**, and the **environment** ***to make access control decisions***.
- Attributes such as **user roles**, **time of access**, **location**, and **data classification** can be considered when ***determining access permissions***.

Protection Models cont…

Access Control Model: Attribute-Based Access Control (ABAC)



Protection Models cont…

Access Control Model: Rule-Based Access Control (RBAC)

- RBAC uses a set of ***predefined rules*** to determine **access permissions**.
- These rules are based on ***conditions*** or ***criteria*** ***specified in policies*** and are ***evaluated to determine*** ***whether access should be granted or denied***.

Protection Models cont…
Access Control Model

- Each Access Control Model has its own advantages and is suitable for different ***security requirements*** and ***environments***.
- Organizations may ***choose to implement*** **one** or a ***combination*** of these models based on their ***specific needs*** and ***risk tolerance***.

Protection Models cont…
Confidentiality Model

- A Confidentiality Model is a security model or framework that focuses on ***protecting the confidentiality of information***.
- It outlines the **measures** and **mechanisms** put in place to ensure that ***sensitive information is only accessible to authorized individuals*** or ***entities*** and ***remains confidential***.

Protection Models cont…
Confidentiality Model

- There are different confidentiality models used in information security, including:

1. Bell-LaPadula Model (BLP)
2. Biba Model
3. Clark-Wilson Model
4. Lattice-Based Model
5. Non-Interference Model

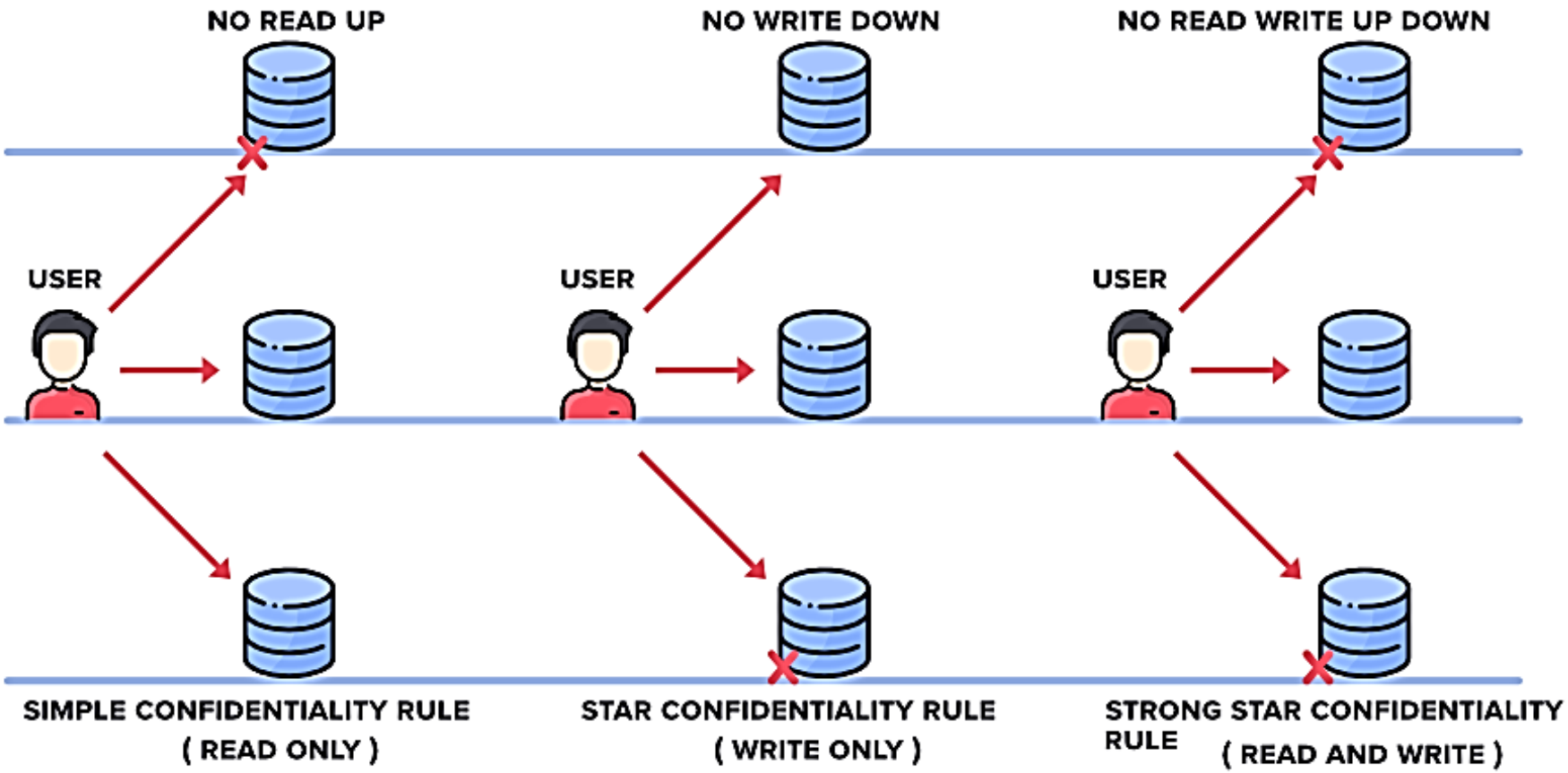
Protection Models cont…

Confidentiality Model: Bell-LaPadula Model (BLP)

- The BLP model is based on the concept of ***multilevel security*** and is primarily used in **government** and **military** contexts.
- It enforces the "**no read up, no write down**" principle, meaning that a user or process ***at a certain security level*** can ***only access or modify*** **information** at that level or lower.

Protection Models cont…

Confidentiality Model: Bell-LaPadula Model (BLP)



Protection Models cont…
Confidentiality Model: Biba Model

- The Biba model, also based on **multilevel security**, focuses on the ***integrity of information***.
- It enforces the "**no write up, no read down**" principle, ensuring that ***information is not modified or accessed*** by ***entities with lower integrity levels***.

Protection Models cont…

Confidentiality Model: Clark-Wilson Model (BLP)

- The Clark-Wilson model is designed to ensure the ***integrity*** ***and*** ***consistency*** of data.
- It emphasizes the use of **well-formed transactions**, **separation of duties**, and **certification of integrity** for data items.

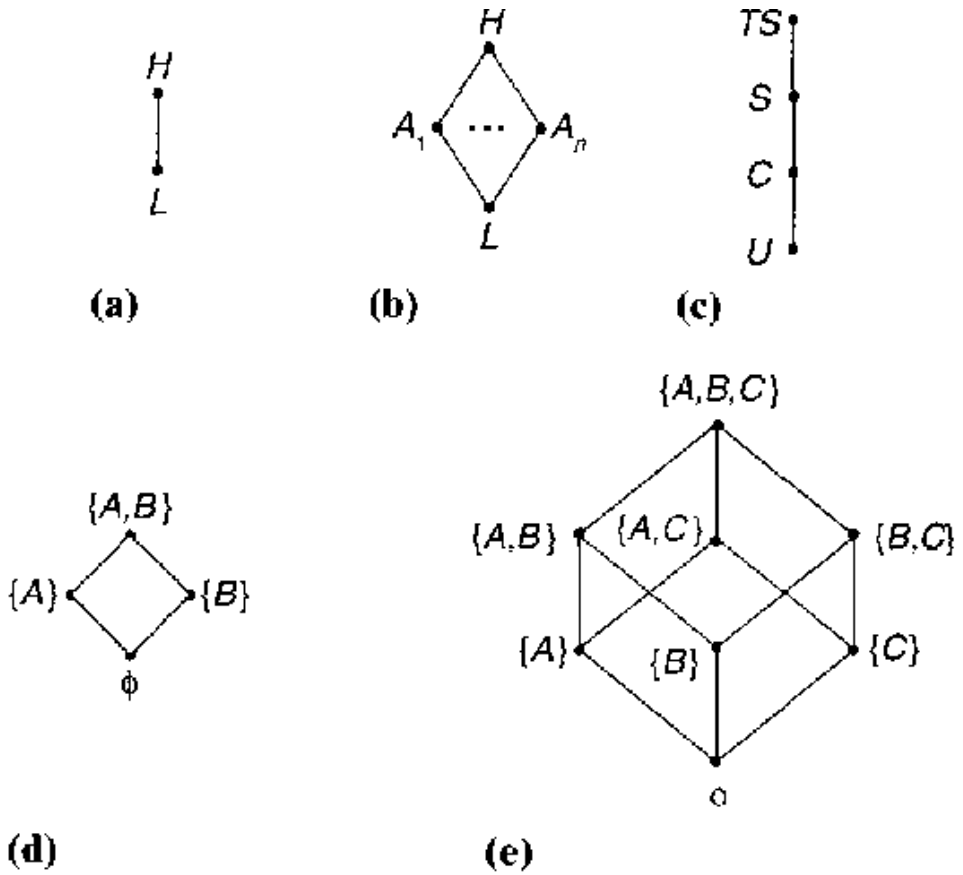
Protection Models cont…

Confidentiality Model: Lattice-Based Model

- The lattice-based model provides a more flexible ***approach to confidentiality*** by ***defining a lattice structure of security levels***.
- It allows for more ***granular access control*** based on the ***sensitivity of information*** and the ***need-to-know principle***.

Protection Models cont…

Confidentiality Model: Lattice-Based Model



Protection Models cont…

Confidentiality Model: Non-Interference Model

- The non-interference model focuses on ***preventing unauthorized information flows*** between **users or processes** with different security levels.
- It aims to ensure that the actions of higher-level users or processes do not interfere with the actions or visibility of lower-level users or processes.

Protection Models cont…
Confidentiality Model

- These confidentiality models, among others, provide guidelines and principles for designing and implementing **security controls** ***to protect sensitive information*** from ***unauthorized disclosure or access***.
- Organizations choose the appropriate confidentiality model based on their specific security requirements, regulatory compliance, and the sensitivity of the information they handle.

Protection Models cont…
Integrity Model

- An Integrity Model in cybersecurity refers to a framework or set of principles that ensures the ***integrity of data and information*** within a system or network.
- The primary objective of an integrity model is to prevent ***unauthorized or unintended modification***, alteration, or corruption of data.

Protection Models cont…
Integrity Model

- There are several integrity models commonly used in information security:

1. Biba Model
2. Clark-Wilson Model
3. Non-Interference Model
4. Brewer-Nash Model (also known as the "CAP Theorem")
5. Trusted Computing Base (TCB) Model

Protection Models cont…
Integrity Model: Brewer-Nash Model

- Brewer-Nash Model also known as the “CAP Theorem”.
- The Brewer-Nash model focuses on the ***trade-off between consistency***, ***availability***, and ***partition tolerance*** in distributed systems.
- It states that it is impossible to achieve all three properties simultaneously in a distributed system.

Protection Models cont…
Integrity Model: Brewer-Nash Model

- While not specifically an integrity model, it helps in understanding the challenges and considerations for maintaining data integrity in distributed environments.

Protection Models cont…

Integrity Model: Trusted Computing Base (TCB) Model

- The TCB model focuses on defining and protecting a trusted computing base, which includes the hardware, software, and firmware components that are essential for system integrity.
- It ensures that critical components are tamper-proof and protected from unauthorized modifications.

Protection Models cont…
Integrity Model

- These integrity models, among others, provide guidelines and mechanisms for ***maintaining the integrity*** of **data** and ensuring that **unauthorized modifications** or **corruption** are **prevented**.
- Organizations adopt the appropriate integrity model based on their specific security requirements, compliance needs, and the nature of the data they handle.

Protection Models cont…
Availability Model

- The Availability Model in cybersecurity refers to a **framework** or **set of principles** that ensure the ***continuous availability*** and ***accessibility*** of **systems**, **networks**, and **resources** to ***authorized users***.
- The primary objective of an availability model is to prevent or mitigate ***disruptions***, ***downtime***, or ***denial-of-service (DoS)*** attacks that ***could impact the availability of critical services***.

Protection Models cont…
Availability Model

- Here are some common elements and considerations in an availability model:

1. Redundancy and Failover
2. Load Balancing
3. Fault Tolerance

Protection Models cont…
Availability Model

4. Disaster Recovery and Business Continuity Planning
5. Distributed Denial-of-Service (DDoS) Mitigation
6. Incident Response and Incident Management
7. Scalability and Capacity Planning
8. Monitoring and Alerting

Protection Models cont…
Availability Model: Redundancy and Failover

- Implementing redundant systems, networks, or components to ensure that **if one fails**, ***another can take over seamlessly***.
- This includes redundant power supplies, network links, servers, and data centers.

Protection Models cont…
Availability Model: Load Balancing

- Distributing **network traffic** or **workload** across multiple servers or systems to ***prevent overloading*** and ***ensure optimal performance***.
- Load balancing helps ***distribute resources effectively*** and ***maintain availability*** during **peak usage**.

Protection Models cont…
Availability Model: Fault Tolerance

- Designing systems with built-in capabilities to **detect** and **recover** ***from failures automatically***.
- This may involve technologies such as ***fault-tolerant hardware***, ***clustering***, or ***replication*** of **critical services**.

Protection Models cont…

Availability Model: Disaster Recovery and Business Continuity Planning

- Developing comprehensive plans and processes to recover systems and services in the event of a major disruption or disaster.
- This includes **data backups**, **off-site storage**, and **predefined procedures** for ***system recovery and business resumption***.

Protection Models cont…

Availability Model: Distributed Denial-of-Service (DDoS) Mitigation

- Implementing measures to **detect and mitigate DDoS attacks**, which aim to ***overwhelm systems or networks*** with a **flood of traffic** or **requests**.
- This may involve **traffic analysis**, **rate limiting**, or ***deploying DDoS protection services***.

Protection Models cont…

Availability Model: Incident Response and Incident Management

- Establishing incident response procedures to **quickly identify** and **respond** to ***incidents that affect availability***.
- This includes **incident detection**, **containment**, **investigation**, and **recovery processes**.

Protection Models cont…

Availability Model: Scalability and Capacity Planning

- Ensuring that systems and infrastructure can **scale up** or **down** to ***handle increasing or fluctuating demands***.
- This involves **monitoring resource utilization**, **capacity planning**, and ensuring **adequate resources are available** ***to meet user demands***.

Protection Models cont…
Availability Model: Monitoring and Alerting

- Implementing robust monitoring systems to **proactively detect and respond** to ***availability issues***.
- This includes real-time monitoring of system health, network performance, and service availability, along with alerting mechanisms to notify administrators of potential issues.

Protection Models cont…
Availability Model

- By adopting an availability model and implementing appropriate measures, organizations can minimize downtime, ensure continuous access to critical services, and mitigate the impact of disruptions or attacks on their systems and networks.

Protection Models

Part 2

Information Security

Arfan Shahzad
{ arfanskp@gmail.com }

Protection Models cont…
Defense in Depth Model

- The Defense in Depth model, also known as **layered security**, is a ***cybersecurity strategy*** that involves **implementing multiple layers of defense** to protect ***systems***, ***networks***, and ***data***.
- The goal is to create ***multiple barriers*** and ***safeguards*** to **prevent or mitigate** the ***impact of security breaches and attacks***.
- Each layer in the Defense in Depth model provides a unique set of security controls and measures, collectively forming a robust and comprehensive security posture.

Protection Models cont…
Defense in Depth Model

Protection Models cont…
Defense in Depth Model

- Here are the key components or layers typically found in a Defense in Depth model:

1. Perimeter Security
2. Network Security
3. Host-based Security

Protection Models cont…
Defense in Depth Model

4. Application Security
5. Data Security
6. User Security
7. Physical Security

Protection Models cont…
Defense in Depth Model: Perimeter Security

- The **outermost layer** focuses on ***securing the network perimeter*** and ***preventing unauthorized access***.
- It involves technologies like **firewalls**, **intrusion detection systems** (IDS), **intrusion prevention systems** (IPS), and **virtual private networks** (VPNs) to control and monitor ***incoming and outgoing traffic***.

Protection Models cont…
Defense in Depth Model: Network Security

- This layer involves **securing** ***internal networks***, ***segments***, and ***communication channels***.
- It includes technologies like network **segmentation**, **VLANs**, **network access control** (NAC), and **network monitoring tools** to ***detect and mitigate network-based threats***.

Protection Models cont…
Defense in Depth Model: Host-Based Security

- This layer focuses on ***securing individual devices***, such as **servers**, **workstations**, and **endpoints**.
- It involves implementing measures like ***antivirus software***, ***host firewalls***, ***endpoint protection***, and ***patch management*** to protect against **malware**, **unauthorized access**, and **vulnerabilities**.

Protection Models cont…
Defense in Depth Model: Application Security

- This layer emphasizes securing **software applications** and their **underlying platforms**.
- It includes practices such as ***secure coding***, ***input validation***, ***access controls***, and ***web application firewalls*** (WAFs) to **prevent** ***common application-level attacks*** like **SQL injections**, **cross-site scripting** (XSS), and **code exploits**.

Protection Models cont…
Defense in Depth Model: Data Security

- This layer focuses on **protecting sensitive data** throughout its ***lifecycle***.
- It involves ***encryption***, ***data loss prevention*** (DLP), ***access controls***, ***data classification***, and ***data backup strategies*** to ensure **confidentiality**, **integrity**, and **availability** of data.

Protection Models cont…
Defense in Depth Model: User Security

- This layer involves securing **user accounts**, **authentication mechanisms**, and **user behavior**.
- It includes measures like ***strong password policies***, ***multi-factor authentication*** (MFA), ***user awareness training***, and ***user access controls*** to mitigate risks associated with **compromised or malicious user accounts**.

Protection Models cont…
Defense in Depth Model: Physical Security

- This layer addresses **physical threats** to the **infrastructure** and **facilities** ***where systems and data reside***.
- It includes measures like ***access control systems***, ***surveillance cameras***, ***security guards***, and ***environmental controls*** to prevent **unauthorized physical access**, **theft**, or **damage**.

Protection Models cont…
Defense in Depth Model

- The Defense in Depth model recognizes that **no single security measure** is **foolproof**, and ***by layering multiple security controls***, ***organizations can create a more resilient and effective defense*** against various threats and attack vectors.
- The idea is that if one layer fails or is bypassed, other layers can provide additional protection, making it more difficult for attackers to penetrate the entire system.

Protection Models cont…
Least Privilege Model

- The Least Privilege Model, also known as the **Principle of Least Privilege** (PoLP), is a ***security principle and access control model*** that restricts ***user privileges to the minimum level necessary to perform their assigned tasks***.
- The goal is to limit the potential damage that can be caused by a compromised or malicious user or application.

Protection Models cont…
Least Privilege Model

- Here are some key principles and benefits of the Least Privilege Model:

1. Principle of Minimal Privilege
2. Segregation of Duties
3. Access Controls
4. Privilege Escalation Mitigation
5. Enhanced Security
6. Compliance Requirements

Protection Models cont…

Least Privilege Model: Principle of Minimal Privilege

- Users are granted the ***minimum set of privileges required*** to ***perform their tasks effectively***.
- This includes access to **systems**, **files**, **networks**, and **administrative functions**.
- By **limiting privileges**, organizations ***reduce the attack surface*** and ***potential damage*** caused by ***unauthorized or malicious actions***.

Protection Models cont…
Least Privilege Model: Segregation of Duties

- The model enforces the **separation of duties** and **responsibilities** among different users or roles.
- It ensures that ***no single individual has complete control*** over **critical functions or resources**.
- This helps **prevent conflicts** of **interest** and ***reduces the risk of insider threats***.

Protection Models cont…
Least Privilege Model: Access Control

- The model emphasizes **implementing strong access controls**, such as ***role-based access control*** (RBAC) or ***attribute-based access control*** (ABAC), to enforce least privilege.
- These controls ensure that **users** can ***only access the resources they specifically require for their tasks*** and that **access permissions** ***are regularly reviewed and updated***.

Protection Models cont…

Least Privilege Model: Privilege Escalation Mitigation

- The model aims to prevent ***privilege escalation attacks***, where an **attacker** ***gains unauthorized access to higher privilege levels***.
- By strictly limiting user privileges, even **if** ***one account is compromised***, the ***potential damage is limited*** to that ***specific user's permissions***.

Protection Models cont…
Least Privilege Model: Enhanced Security

- The Least Privilege Model improves overall system security by ***reducing the attack surface*** and ***limiting the impact of potential security breaches***.
- It helps prevent **unauthorized access**, **privilege misuse**, **malware propagation**, and **lateral movement** within the network.

Protection Models cont…

Least Privilege Model: Compliance Requirements

- Many industry regulations and frameworks, such as **Payment Card Industry Data Security Standard** (PCI DSS) and, **Health Insurance Portability and Accountability Act.** (HIPAA), mandate the implementation of the Least Privilege Model as a **security best practice**.
- Adhering to this model helps organizations meet ***compliance requirements*** and ***demonstrate a commitment*** to **protecting sensitive data**.

Protection Models cont…
Principle of Least Astonishment (POLA) Model

- In the context of cybersecurity, the "**Principle of Least Astonishment**" (POLA) is a guiding principle that **focuses** on ***minimizing surprises*** and ***unexpected behaviors*** in security systems and protocols.
- It aims to design security measures and controls in a way that ***aligns with users' expectations*** and ***minimizes confusion*** or ***misunderstandings***.

Protection Models cont…
Principle of Least Astonishment (POLA) Model

- The POLA model in cybersecurity emphasizes the following:
- **1- User-Friendly Interfaces:** Security systems should have user interfaces that are **intuitive** and **easy to use**, **reducing the chances of user errors** or **unintended actions**.
- Clear and concise ***instructions***, as well as ***familiar design elements***, **can help** ***users understand*** and ***navigate security measures effectively***.

Protection Models cont…
Principle of Least Astonishment (POLA) Model

- **2- Transparent Security Controls:** Security mechanisms should be **transparent** to users to the extent possible.
- Users should have a ***clear understanding*** of the ***security measures in place*** and ***their implications***.
- Any ***unexpected behaviors*** or ***prompts*** **should be minimized**, ensuring that ***users are not caught off guard*** or ***confused***.

Protection Models cont…
Principle of Least Astonishment (POLA) Model

- **4- Balance between Security and Usability:** The POLA model recognizes the need ***to find a balance between security and usability***.
- The goal is to implement security measures that are effective yet user-friendly.