جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

قسم الامن السيبراني

Department of Cyber Security

Subject: Principles of Cyber Security

Class: 1st

Lecture: (2)

Basics of System Security and User Access Control

Lecturer: Msc :Najwan thaeer ali

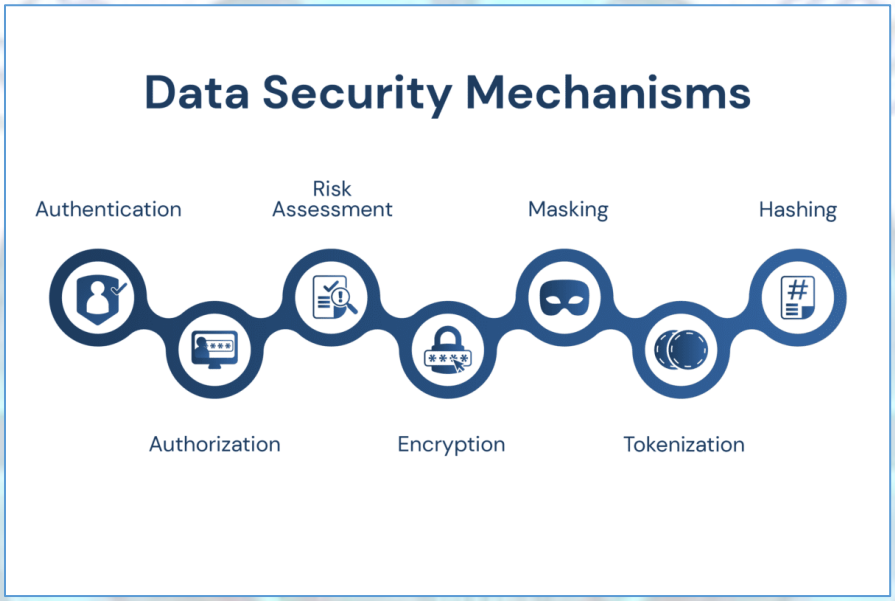
Introduction

System security is essential for protecting data and resources from unauthorized access. This lecture introduces the basic concepts of authentication, chain of authority, and access control, which are used to manage user identities and permissions. Understanding these concepts helps ensure secure and organized access to information systems.

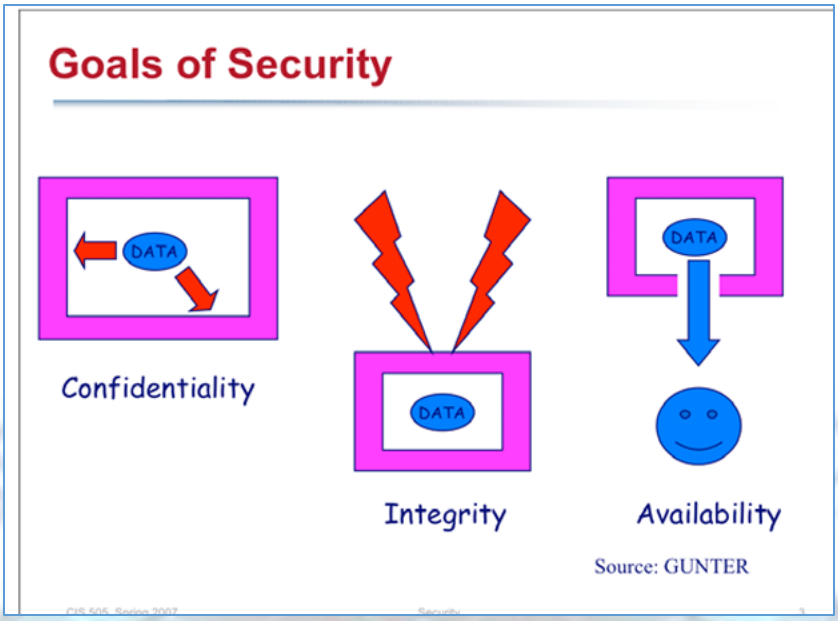
Security and Access Control Models نماذج الأمن والتحكم بالوصول

1. **Security mechanisms**
2. **Authentication**
3. **Chain of Authority**
4. **Access control**
5. **Permissions-based access control.**

1-Security Mechanisms:Security mechanisms are techniques and procedures used to protect systems and data.



- Main Goals:
- - Confidentiality
- - Integrity
- - Availability



- **Examples:**

- Encryption- Firewall- Intrusion Detection Systems

2-Authentication:Authentication is the process of verifying the identity of a user.

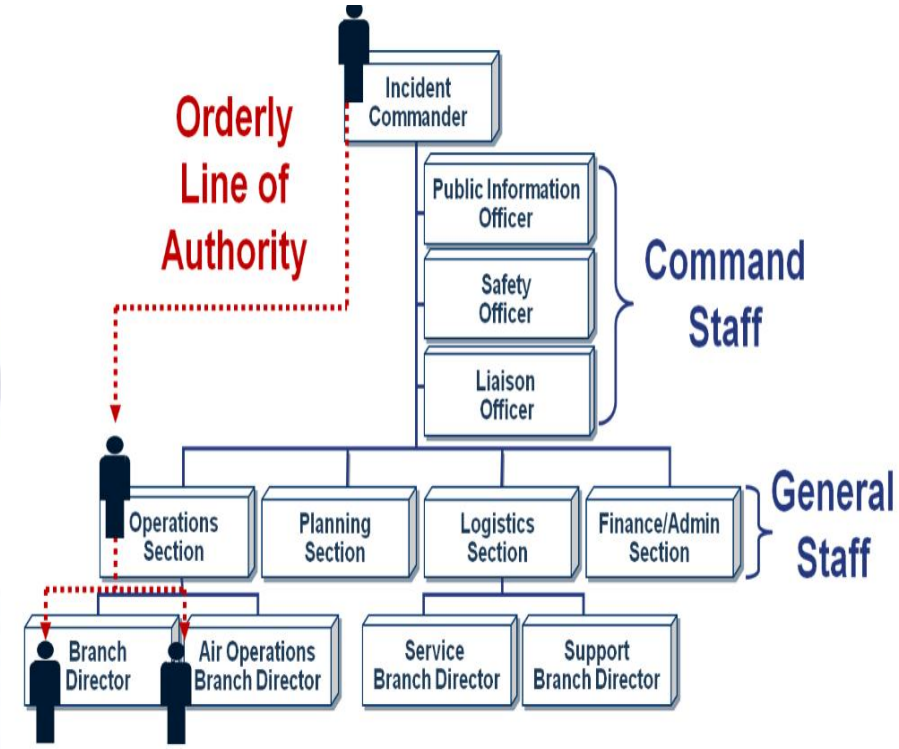
Types of Authentication:

Something you know (password)
Something you have (smart card, phone)
Something you are (fingerprint, face recognition)

Importance:

Prevents identity theft

3-Chain of Authority: Chain of Authority defines a hierarchical structure of permissions within a system.



Features:

1. Clear hierarchy of roles
2. Defined responsibilities

Example:

System Administrator→Manager → User

4-Access Control: Access control determines who can access resources and how.

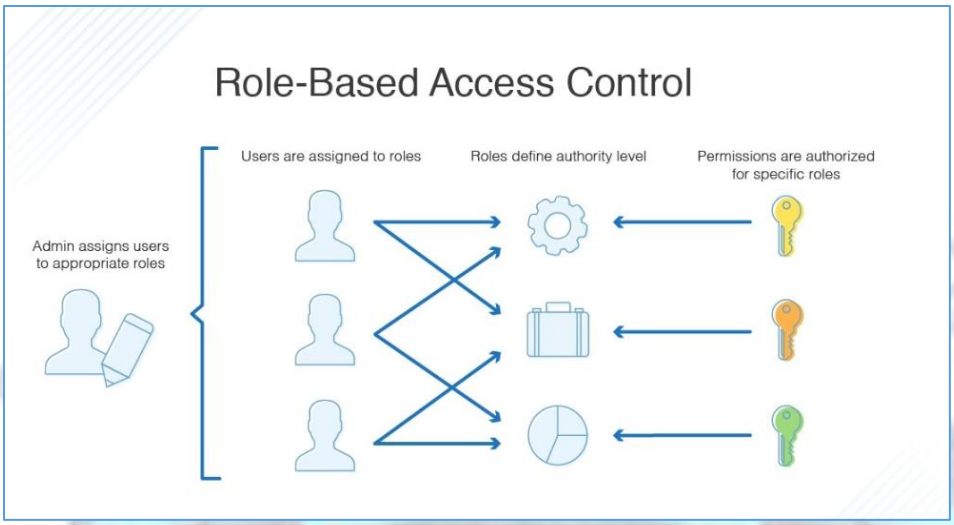
Types:

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Role-Based Access Control (RBAC)

Example:

Students can view files, instructors can edit them

5-Permissions-Based Access Control: This model grants users specific permissions.



Common Permissions:

Read- Write- Execute

Advantages:

High flexibility- Reduced security risks

- Example:

User can read a file but cannot modify it

Refrance:

1-NIST – National Institute of Standards and Technology
Access Control Concepts and Technologies.

2-OWASP Foundation
Authentication and Access Control Documentation.

3-IBM Security Documentation
Authentication ;Authorization**.**