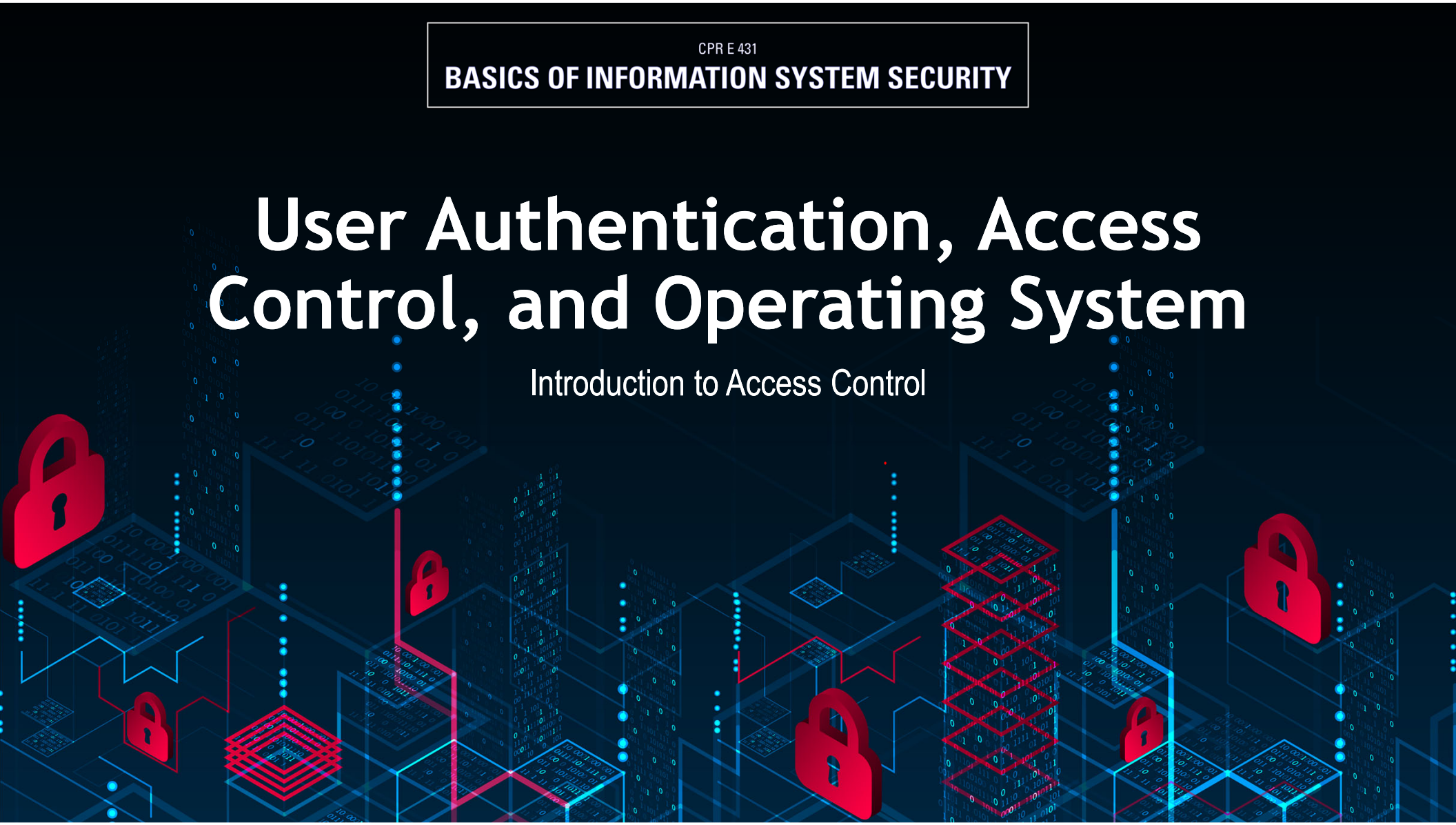
CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

User Authentication, Access Control, and Operating System

Introduction to Access Control



Video Summary

- What is Access Control (AC)
- Subjects, Objects, and Access Rights
- General Requirements of Access Control

Access Control Definitions 1/2

NIST 7298 defines access control as:

"The process of granting or denying specific requests to:

(1) obtain and use information and related information processing services
(2) enter specific physical facilities"

Access Control Definitions 2/2

RFC 4949 defines access control as:

> "A process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy"

Access Control Principles

- In a broad sense, all of computer security is concerned with access control

- RFC 4949 defines computer security as:

> "measures that implement and assure security services in a computer system, particularly those that assure access control service"

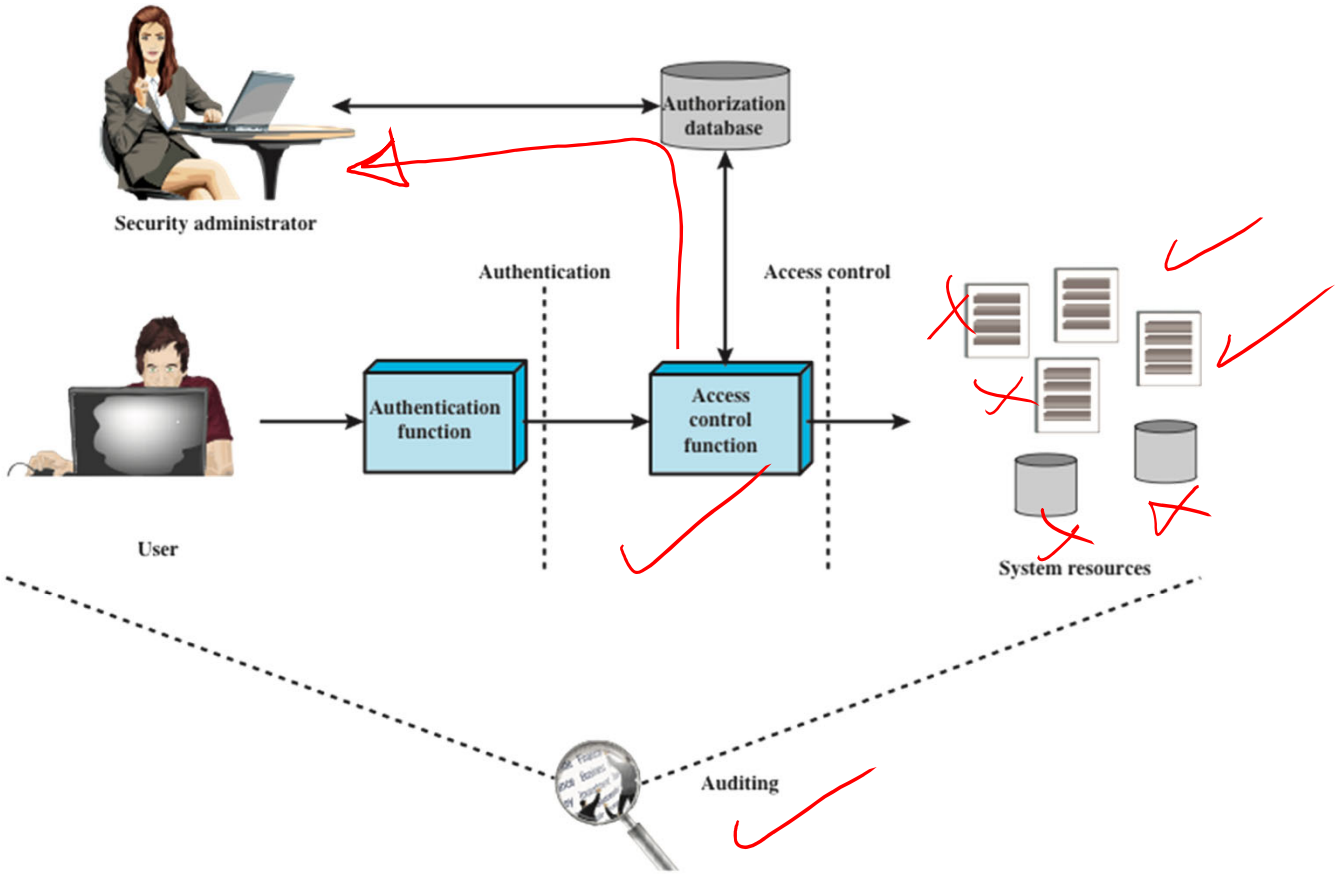
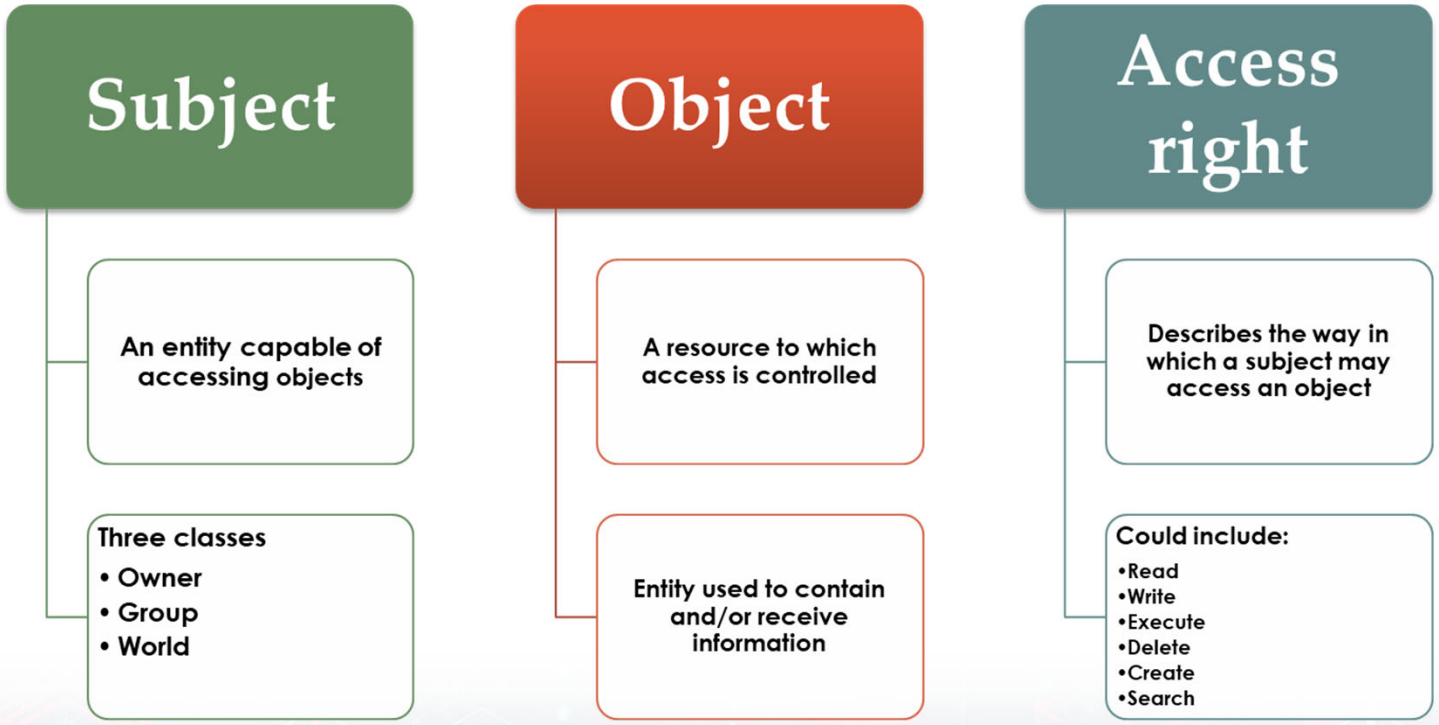


Figure 4.1 Relationship Among Access Control and Other Security Functions

Access Control & Security Functions

Authentication	verification that the credentials of a user or other entity are valid
Authorization	granting of a right or permission to a system entity to access a resource
Audit	independent review of system records and activities in order to test for adequacy of system control, ensure compliance to policy, detect breaches and recommend changes

Subjects, Objects, and Access Rights



General Requirements of Access Control

- Reliable input
- Fine and coarse specifications
- Least privilege
- Separation of duty
- Open and closed policies
- Policy combinations and conflict resolution
- Administrative policies
- Dual control

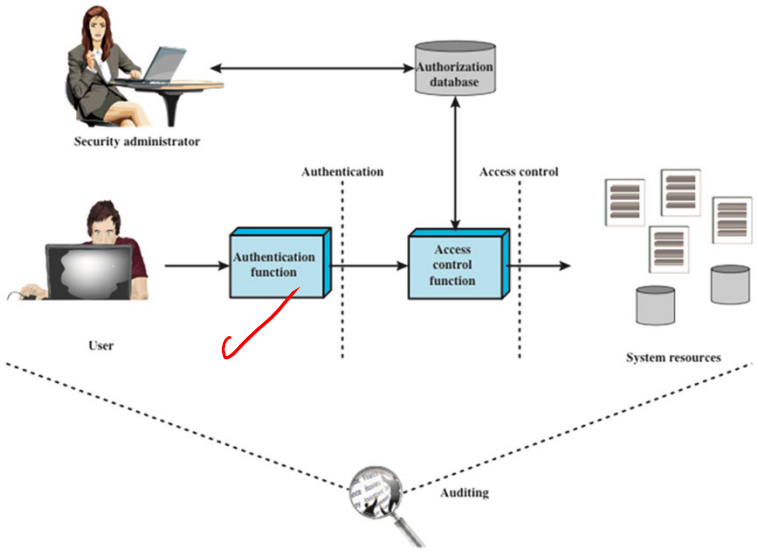


Figure 4.1 Relationship Among Access Control and Other Security Functions

Access Control Policies

- Discretionary access control (DAC)
  - Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do
- Mandatory access control (MAC)
  - Controls access based on comparing security labels with security clearances
- Role-based access control (RBAC)
  - Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles

Video Summary

- What is Access Control (AC)
- Subjects, Objects, and Access Rights
- General Requirements of Access Control