Network Defense Essentials

Module 02

Identification, Authentication, and Authorization

Module Objectives

- Understanding the Terminology, Principles, and Models of Access Control
- Understanding Identity and Access Management (IAM)
- Understanding User Access Management
- Overview of Different Types of Authentication
- Overview of Different Types of Authorization
- Understanding User Accounting

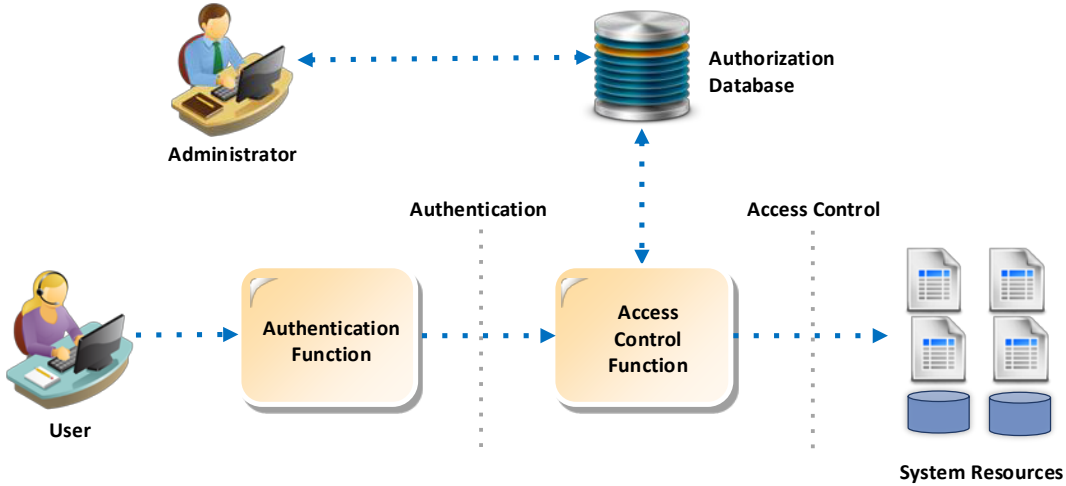
Module Flow

Discuss Access Control Principles, Terminologies, and Models 1

Discuss Identity and Access Management (IAM) Concepts 2

Access Control

- Access control is the **selective restriction** of access to an asset or a system/network resource
- It **protects the information assets** by determining who can access what
- Access control mechanism uses **user identification**, **authentication**, and **authorization** to restrict or grant access to a specific asset/resource



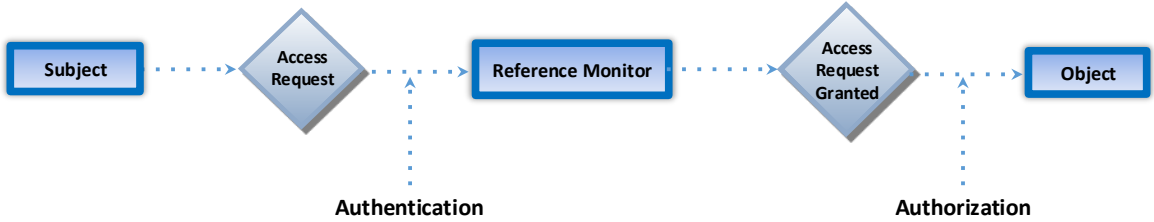
Access Control Terminologies

Subject — This refers to a **particular user** or **process** that wants to access a resource

Object — This refers to a **specific resource** that the user wants to access such as a file or a hardware device

Reference Monitor — It checks the **access control rule** for specific restrictions

Operation — It represents an **action** taken by a subject on an object



Access Control Principles

Separation of Duties (SoD)

- Involves a breakdown of the authorization process into various steps
- Different privileges are assigned at each step to the individual subjects requesting for a resource
- This ensures that no single individual has the authorization rights to perform all functions and simultaneously denies access of all the objects to a single individual

Need-to-know

- Under the need-to-know access control principle, access is provided only to the information that is required for performing a specific task

Principle of Least Privilege (POLP)

- Principle of least privilege extends the need-to-know principle in providing access to a system
- POLP believes in providing employees a need–to-know access, i.e., not more, not less;
- It helps an organization by protecting it from malicious behavior, achieving better system stability, and system security

Access Control Models

- Access control models are the **standards which provide a predefined framework** for implementing the necessary level of access control

Mandatory Access Control (MAC)

- ✓ Only the administrator/system owner has the rights to assign privileges
- ✓ It does not permit the end user to decide who can access the information

Discretionary Access Control (DAC)

- ✓ End user has complete access to the information they own

Role-based Access Control (RBAC)

- ✓ Permission are assigned based on user roles

Rule-based Access Control (RB-RBAC)

- ✓ Permissions are assigned to a user role dynamically based on a set of rules defined by the administrator

Mandatory Access Control

The mandatory access control (MAC) determines the usage and access policies for the users. A user can access a resource only if they have the access rights to that resource. MAC is applied in the case of data that has been marked as highly confidential. The administrators impose MAC depending on the operating system and the security kernel.

The following are the advantages and disadvantages of MAC:

- It provides a high level of security since the network defenders determine the access controls.
- The MAC policies minimize the chances of errors.
- Depending on the MAC, an operating system marks and labels the incoming data, thereby creating an external application control policy.

Examples of MAC include Security-Enhanced Linux (SELinux) and Trusted Solaris

Discretionary Access Control

Discretionary access control **(DAC)** determines the access control taken by any possessor of an object in order to decide the access control of a subject on that object. DAC is alternatively named as a **need-to-know** access model. The decision taken by the owner depends on the following measures:

- **File and data ownership**: Determines the access policies of the user
- **Access rights and permissions**: Involves the possessor setting the access privileges to other subjects

An owner can provide or deny access to any particular user or a group of users. The attributes of a DAC include the following:

- The owner of an object can transfer the ownership to another user.
- The access control prevents multiple unauthorized attempts to access an object.
- The DAC prevents unauthorized users from viewing details like the filesize, filename,
- The DAC uses access control lists in order to identify and authorize users.

Disadvantage: A DAC requires maintenance of the access control list and access permissions for the users. Examples of DAC include UNIX, Linux, and Windows access control.

Role-Based Access Control

In a role-based access control **(RBAC)**, the access permissions are available based on the access policies determined by the system. The access permissions are beyond the user control which implies that users cannot amend the access policies created by the system. The rules for determining the role-based access controls are as follows:

- **Role assignment:** A certain role is required to be assigned to a user which enables them to perform a transaction.
- **Role authorization:** A user needs to perform a role authorization in order to achieve a particular role.
- **Transaction authorization:** Transaction authorization allows the users to execute only those transactions for which they have been authorized.

Rule-based Access Control (RB-RBAC)

Permissions are assigned to a user role dynamically based on a set of rules defined by the administrator.

important

Example of the MAC Model: Bell-LaPadula Model (BLM)

الأكثر شيوعاً بالقطاع العسكري

The Bell-LaPadula (BLP) model is a computer security model which focuses on data confidentiality and controlled access to classified information. The main aim of the BLP model is to prevent users from accessing information above their security level. The BLP model includes aspects of DAC and MAC to integrate confidentiality. It is a static model in which the security levels (labels) never change. This security model uses an access matrix and defines a "no read-up", "no write-down" policy. A layered classification scheme of this model is used for the subjects and a layered categorization scheme is used for the objects. The classification level of the objects and the access rights of the subjects decide the access authorization from the subjects to the objects.

The BLP model consists of two MAC rules with two security properties:

- **Simple security property— no read-up:** A subject at a given security level cannot read an object at a higher security level.
- ***-property— no write-down:** A subject at a given security level cannot write to any object at a lower security level.

The concept of trusted subjects enables the transfer of information from a high-sensitivity document to a lower-sensitivity document.

Limitations of the BLP Model:

- It only addresses confidentiality, control of writing, *-property, and discretionary access control.
- The mentioned covert channels are not addressed comprehensively.
- Limitation of tranquility principle allows a controlled copying from a high security level to a low security level via trusted subjects.

الوسيط او اللي ينقل الـ Subject
لازم يكون موثوق

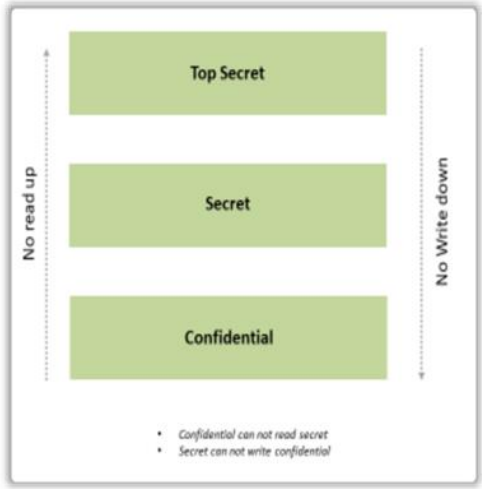


Figure 3.3: Bell-LaPadula (BLP) Model

Example of the MAC Model: Biba Integrity Model

The Biba model/Biba integrity model was developed by Kenneth J. Biba in 1975 and addresses the issue of integrity. The data and subjects are grouped into ordered levels of integrity. This model believes in read-up, write-down, and is the exact opposite of the BLP model.

Figure 3.4: Biba Integrity Model

The Biba model focuses on information integrity and a new label is used for this. In this model, users can only create content at or below their own integrity level and can only view content at or above their own integrity level. This model specifies three integrity axioms:

- **Simple integrity axiom— no read-down:** A subject at a given level of integrity must not read data at a lower integrity level.
- ***** **integrity axiom— no write-up:** A subject at a given level of integrity must not write to data at a higher level of integrity.
- **Invocation axiom:** A subject at one level of integrity cannot invoke a subject at a higher level of integrity.

كل واحد مسؤول عن معلوماته

This model consists of the following access modes:

- **Modify:** Allows a subject to write to an object.
- **Observe:** Allows a subject to read an object.
- **Invoke:** Allows a subject to communicate with another subject.
- **Execute:** Allows a subject to execute an object.

The Biba model is a set of mandatory and discretionary policies.

- The mandatory policies are as follows:
  - **Strict integrity policy:** Enforces "no write-up" and "no read-down" on the data in the system.
  - **Low-watermark policy for subjects:** The low-watermark policy for subjects allows subjects to read-down.
  - **Low-watermark policy for objects:** The low-watermark policy for objects allows subjects to write-up.
  - **Ring policy:** Allows any subject to observe any object.
- **Discretionary policies:** Access control lists and object hierarchy

Example of the DAC Model: Access Control Matrix

The DAC decides the access rights of users simply on the basis of the access control matrix. This matrix is a two-dimensional array in which the subjects are placed against the objects. It characterizes the rights of the subjects with respect to the objects in the system. It is a rectangular array of cells with one row per subject and one column per object. Each entry of a subject-object pair is the access mode that the subject is allowed to exercise on the object. Columns act as the access control list for the object and rows act as the access profile for the subjects.

For example,

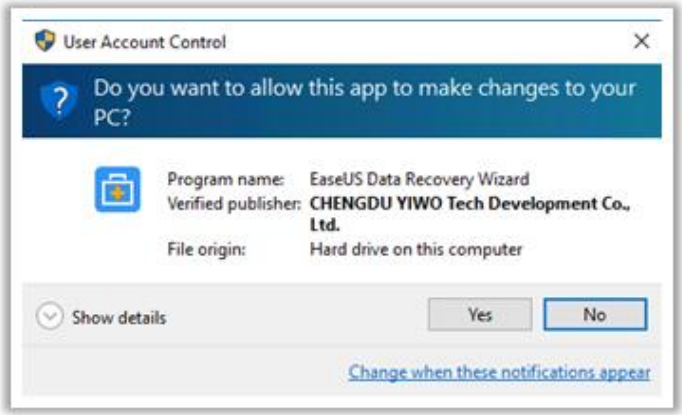
	Object 1	Object 2	Object 3
Subject 1	Own Read Write		Read Write
Subject 2	Read	Own Read Write	read
Subject 3	Read Write	Read	Read Write

Figure 3.5: Access Control Matrix's Two-Dimensional Rectangular Array

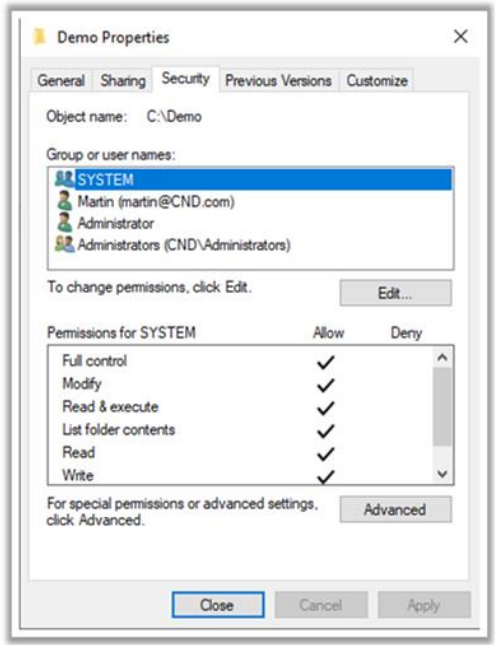
Logical Implementation of DAC, MAC, and RBAC

- Logical implementation of access control is performed using **access control lists (ACLs)**, **group policies**, **passwords**, and **account restrictions**

MAC Implementation: The User Account Control (UAC) tool of Windows OS

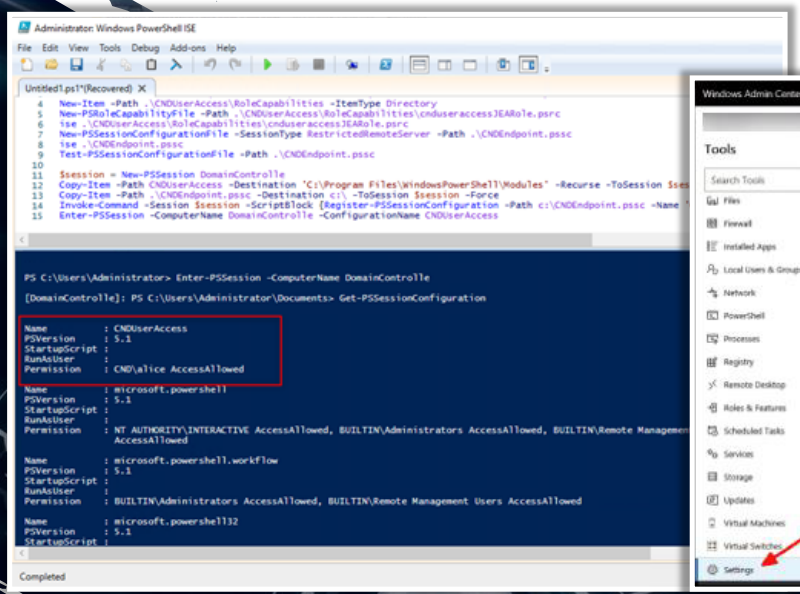


DAC Implementation: Windows File Permissions

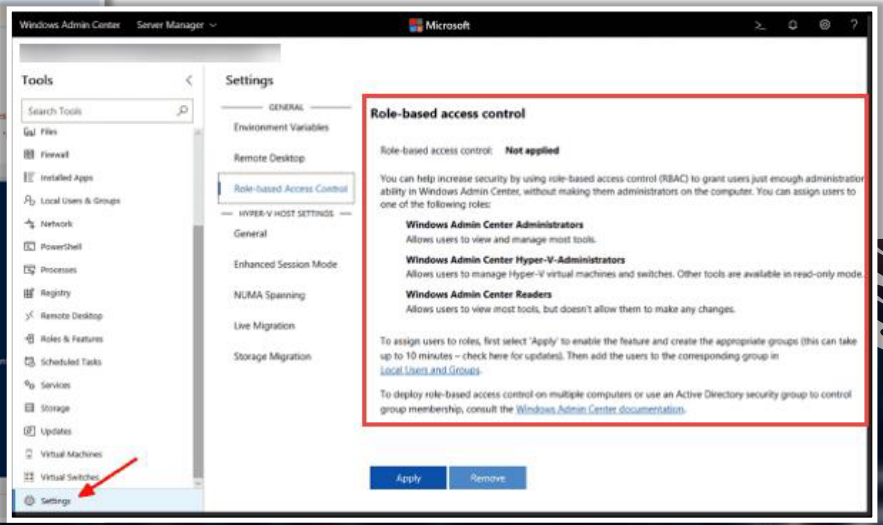


Logical Implementation of DAC, MAC, and RBAC (Cont'd)

RBAC Implementation: Just Enough Administration (JEA)



RBAC Implementation: Windows Admin Center (WAC)

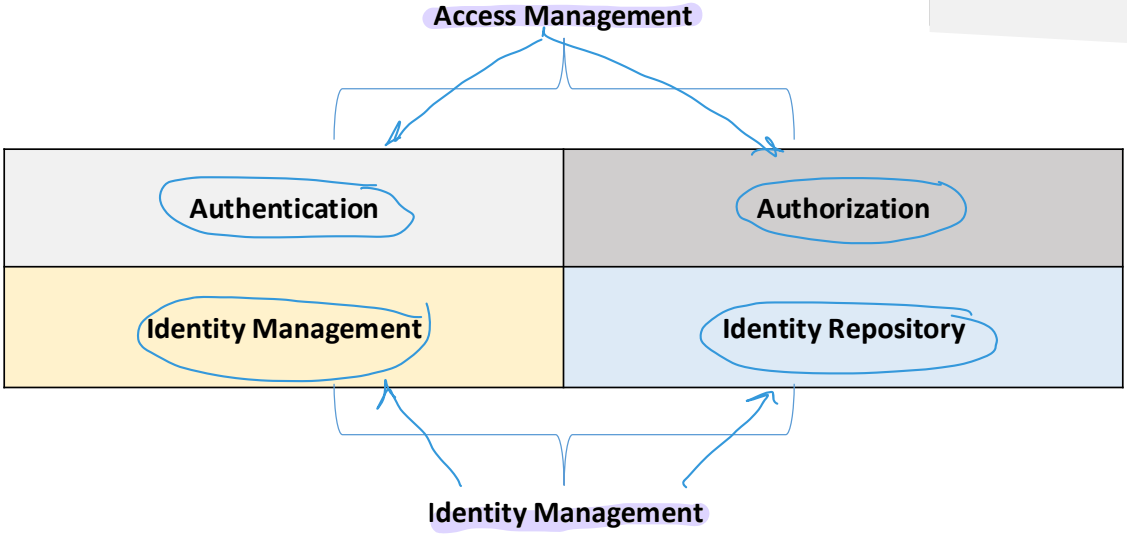


Module Flow

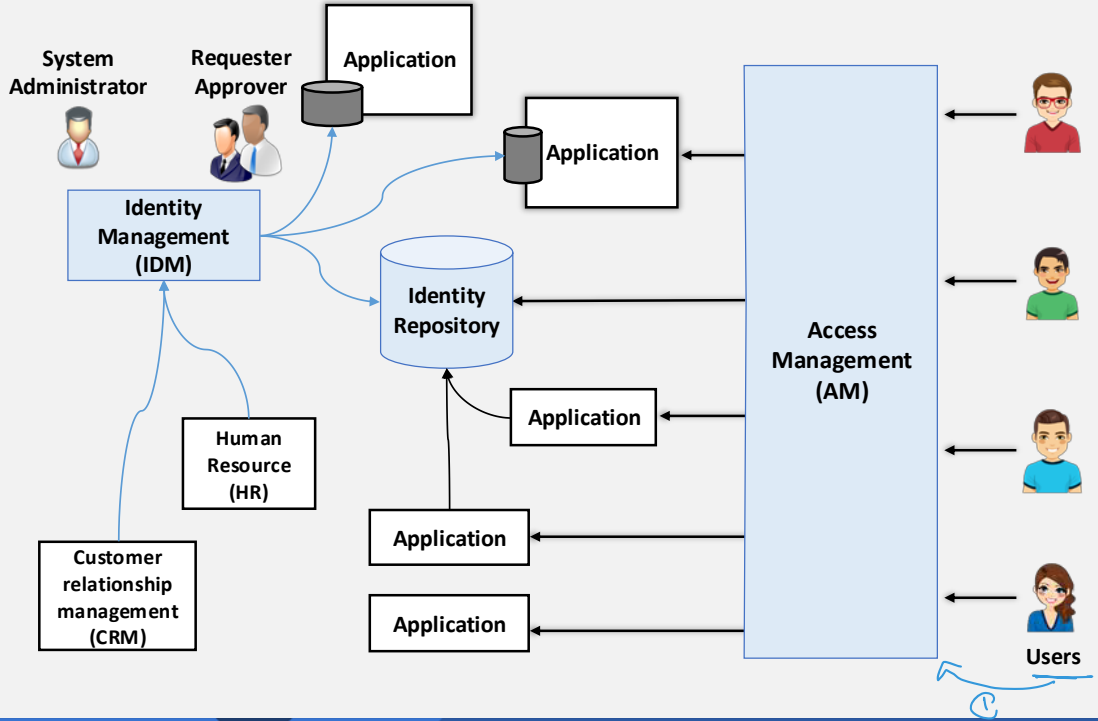
1. Discuss Access Control Principles, Terminologies, and Models
2. Discuss Identity and Access Management (IAM) Concepts

Identity and Access Management (IAM)

- IAM is responsible for providing the **right individual with right access at the right time**



Identity and Access Management (IAM) (Cont'd)



User Identity Management (IDM)

Identity Management

- ✓ User Identification involves a method to ensure that an **individual holds a valid identity**
- ✓ Examples of user identity includes attributes such as a username, account number, user roles, etc.
- ✓ Identify Management involves storing and managing user attributes in their repositories

Identity Repository

- ✓ The user repository is a database where attributes related to the users' identities are stored

User Access Management (AM): Authentication

- Authentication involves validating the **identity of an individual with a system**, **application**, or **network**

Types of Authentication

- **Password Authentication**
- **Smart Card Authentication**
- **Biometric Authentication**
- **Two-factor Authentication**
- **Single Sign-on (SSO) Authentication**

Types of Authentication

multi factor
- You know
- You have
- You are

Password Authentication

- Password Authentication uses a **combination** of a username and a password to authenticate the network users
- The password is checked against a **database** and the user is given access if it matches
- Password authentication can be vulnerable to **password cracking attacks** such as brute force or dictionary attacks

Types of Authentication (Cont'd)

Smart Card Authentication

- Smart card is a small **computer chip device** that holds a users' personal information required to authenticate them
- Users have to insert their smart cards into the card reader machines and enter their **personal identification number** (PIN) to authenticate themselves
- Smart card authentication is a **cryptography-based authentication** and provides stronger security than password authentication

Types of Authentication (Cont'd)

Biometric Authentication

Biometrics refers to the **identification of individuals** based on their physical characteristics

Biometric Identification Techniques

Fingerprint Scanning

Compares two fingerprints for verification and identification on the basis of the patterns on the finger

Retinal Scanning

Analyzes the layer of blood vessels at the back of their eyes to identify a person

Iris Scanning

Analyzes the colored part of the eye suspended behind the cornea

Vein Structure Recognition

Analyzes thickness and location of veins to identify a person

Face Recognition

Uses facial features to identify or verify a person

Voice Recognition

Uses voice patterns to identify or verify a person

Types of Authentication (Cont'd)

Two-factor Authentication

1. Two-factor authentication involves using two different authentication factors out of three (something you know, something your have, and something you are) to verify the **identity of an individual** in order to enhance the **security in authentication systems**

2. **Combinations of two-factor authentication:** password and smart card/token, password and biometrics, password and one-time password (OTP), smart card/token and biometrics, etc.

3. "Something you are" is the best companion of two-factor authentication as it is considered as the **hardest to forge** or **spoof**

Types of Authentication (Cont'd)

Single Sign-on (SSO) Authentication

- It allows a user to authenticate themselves to **multiple servers** on a network with a **single password** without re-entering it every time

Advantages

01. No need to remember passwords of multiple applications or systems
02. Reduces the time for entering a username and password
03. Reduces the network traffic to the **centralized server**
04. Users need to enter credentials only once for multiple applications

User Access Management (AM): Authorization

- Authorization involves **controlling the access** of information for an individual (E.g.: A user can only read a file, but not write in it or delete it)

Types of Authorization Systems

Centralized Authorization

- ✓ Authorization for network access is done using a **single centralized** authorization unit
- ✓ It maintains a **single database** for authorizing all the network resources or applications
- ✓ It is an **easy and inexpensive** authorization approach

Decentralized Authorization

- ✓ Each network resource maintains its **authorization unit** and performs authorization locally
- ✓ It maintains its **own database** for authorization

Implicit Authorization

- ✓ Users can access the requested resource **on behalf** of others
- ✓ The access request goes through a **primary resource** to access the requested resource

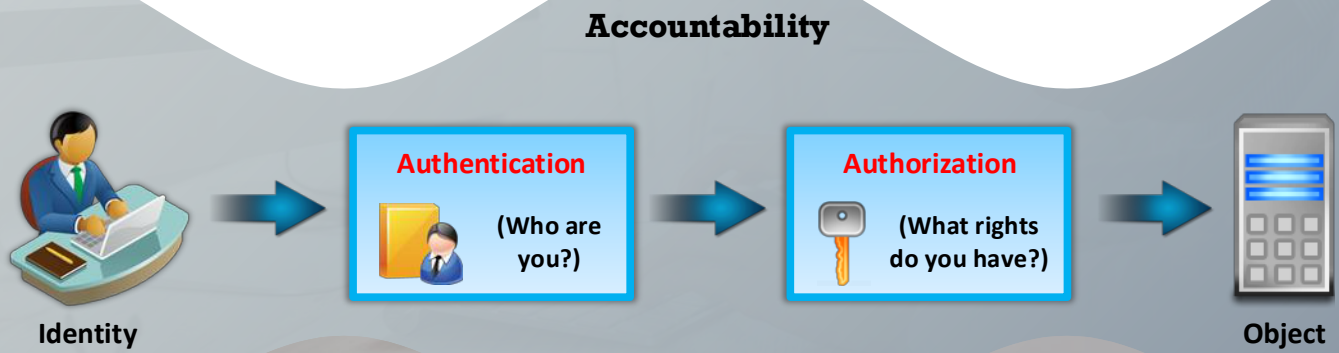
Explicit Authorization

do You allow the camera?

- ✓ Unlike implicit authorization, explicit authorization requires **separate authorization** for each requested resource
- ✓ It explicitly maintains authorization for each **requested object**

User Access Management (AM): Accounting

- Accounting is a method of keeping **track** of **user actions** on the network. It keeps track of who, when, and how the users access the network.
- It helps in identifying authorized and unauthorized actions
- The account data can be used for trend analysis, data breach detection, forensics investigations, etc.



Module Summary

- This module has discussed the access control principles, terminologies, and models
- It has discussed identity and access management concepts
- It also discussed different methods used for user access management
- It has discussed different types of authentication and authorization techniques
- Finally, this module ended with an overview of user accounting and accountability
- In the next module, we will discuss in detail on network security controls - administrative controls