

Access Control

By

Prof. Muhammad Iqbal Bhat

Department of Higher Education,
Government Degree College
Beerwah

Prof. M. Iqbal Bhat (JKHED)



Topics



WHAT IS ACCESS
CONTROL?



TYPES OF ACCESS
CONTROL



AUTHENTICATION
AND AUTHORIZATION



ACCESS CONTROL
MODELS



IMPLEMENTATION OF
ACCESS CONTROL

Prof. M. Iqbal Bhat (JKHED)

Recent access control security breaches

Date	Company/Institution	Type of Breach	Impact
July 2021	Microsoft	Azure AD	Hackers exploited a vulnerability in Microsoft's Azure Active Directory to access customer data
May 2021	Colonial Pipeline	Ransomware Attack	Attackers gained access to the company's network and shut down fuel pipelines
Dec 2020	SolarWinds	Supply Chain Attack	Hackers inserted malicious code into SolarWinds' Orion software, affecting numerous organizations
July 2020	Twitter	Social Engineering	Attackers tricked employees into revealing their credentials, allowing access to high-profile accounts
May 2020	EasyJet	Cyber Attack	Attackers gained access to the personal data of millions of customers
Dec 2019	Travelex	Ransomware Attack	Attackers gained access to the company's network and demanded a ransom
July 2019	Capital One	Insider Threat	A former employee of the bank gained unauthorized access to customer data and was arrested
May 2019	WhatsApp	Vulnerability Exploit	Attackers exploited a vulnerability in the messaging app to install spyware on users' phones

Access Control:

Access control is a fundamental concept in cybersecurity that refers to the process of controlling access to resources and systems based on predefined policies and rules.

Access control is crucial for protecting sensitive data, preventing unauthorized access, and ensuring compliance with regulations and industry standards.

Access control can be classified into different types based on the resources being protected, such as physical, logical, or administrative.

Access control is typically achieved through the process of authentication and authorization, which involves verifying users' identities and granting them access based on their roles, permissions, or clearance levels.

Types of Access Control:



Physical Access Control



Logical Access Control



Administrative Access Control

Physical Access Control:



Physical access control refers to the use of physical barriers, such as locks, security guards, or surveillance systems, to control access to physical resources, such as buildings, rooms, or storage areas.



Examples of physical access control include:

Access cards: Employees use access cards to gain entry to secure areas.

Biometric scanners: Fingerprint scanners or retinal scanners can be used to grant access to restricted areas.

Security guards: Trained security personnel can monitor access to secure areas and prevent unauthorized entry.

Logical Access Control:

Logical access control refers to the use of digital or electronic methods, such as passwords, encryption, or firewalls, to control access to digital resources, such as computer systems, networks, or data.



Examples of logical access control include:

Passwords: Users must enter a unique username and password to gain access to their account or system.

Two-factor authentication: Users must provide two forms of identification, such as a password and a token, to gain access to a system.

Firewalls: Network firewalls can be used to restrict access to certain ports or IP addresses, preventing unauthorized access to a network.

Administrative Access Control:

Administrative access control refers to the use of policies, procedures, and rules to control access to administrative resources, such as systems, networks, or applications.



Examples of administrative access control include:

Role-based access control (RBAC): Users are assigned specific roles, which determine their access to resources and functions.

Mandatory access control (MAC): Access is determined by a security clearance level, which is assigned by an administrator based on an employee's job function and level of trust.

Discretionary access control (DAC): Access is granted at the discretion of the resource owner, who decides which users are allowed to access their resources:

How is access control achieved:

Access control is typically achieved through the process of authentication and authorization, which involves verifying users' identities and granting them access based on their roles, permissions, or clearance levels.

Authentication:

Authentication is the process of verifying a user's identity to ensure that only authorized users are granted access to resources.

Authentication can be achieved through different methods, such as passwords, biometric scans, smart cards, or tokens.

Authentication is critical for ensuring the confidentiality and integrity of sensitive data, as it helps prevent unauthorized access and potential data breaches.

Authentication methods can be classified into three categories:

- knowledge-based,
- possession-based
- biometric-based.

Knowledge-based authentication:

Knowledge-based authentication (KBA) relies on information that the user knows, such as a password, passphrase, or PIN.

Examples of knowledge-based authentication include:

Passwords: Users are required to create a unique password that they must enter to access their account or system.

Passphrases: Similar to passwords, but they are typically longer and include spaces between words.

PINs: Users enter a numeric code to gain access to a system or device.

Possession-based authentication

Possession-based authentication relies on something the user possesses, such as a smart card, token, or key

Examples of possession-based authentication include

Smart cards: Users are issued a smart card that they must present to a card reader to gain access to a secure area or system.

Tokens: Similar to smart cards, but they generate a unique code that the user must enter to gain access to a system or application.

Keys: Physical keys can be used to access secure areas or devices, such as lockers or server racks.

Biometric-based authentication:

Biometric-based authentication relies on physical characteristics unique to the user, such as fingerprints, facial recognition, or iris scans.

Examples of biometric-based authentication include

Fingerprint scanners: Users place their finger on a scanner to verify their identity.

Facial recognition: Users take a selfie or scan their face to verify their identity.

Iris scans: Similar to fingerprint scanners, but they scan the user's iris instead of their fingerprint.

Authorization:

Authorization is the process of granting or denying access to resources based on a user's identity, role, or permission level.



Authorization can be based on different factors, such as job function, clearance level, or access policies.



Authorization is critical for ensuring that users only have access to the resources they need to perform their job functions, and no more, which helps prevent data leaks and minimize the impact of potential security incidents.

Prof. M. Isha Bhat (JKHED)

Authorization:


**role-based
authorization**

**attribute-based
authorization.**

Prof. M. Iqbal Bhat (JKHED)

Role-based authorization:

Role-based authorization (RBAC) grants access to resources based on a user's job function or role within the organization.



Examples of role-based authorization include:

Employee roles: Different employee roles have different levels of access to resources based on their job function, such as managers, executives, or customer service representatives.

User groups: Users can be grouped together based on their job function or department, and access to resources can be granted based on group membership.

Privilege levels: Users can be granted different levels of access to resources based on their role or job function, such as read-only access, edit access, or admin access.

Attribute-based authorization:

Attribute-based authorization (ABAC) grants access to resources based on specific attributes or characteristics of the user or resource being accessed.

Examples of attribute-based authorization include:

User attributes: Access to resources can be granted or denied based on user attributes such as location, department, or security clearance level.

Resource attributes: Access to resources can be granted or denied based on resource attributes such as sensitivity level, data classification, or data type.

Contextual attributes: Access to resources can be granted or denied based on contextual attributes such as time of day, location, or device being used.

Access Control Models:

Access control models are used to define the rules and policies that govern access to resources within an organization.



Access control models can be classified into three categories:

**discretionary
access control**

**mandatory
access control**

**role-based
access
control.**

Discretionary Access Control (DAC):



Discretionary access control (DAC) is a type of access control where the owner of a resource has complete control over who is granted access to it.



Examples of DAC include:

File permissions: Users can grant or deny access to files or folders on their personal computer.

Group permissions: Users can grant or deny access to resources based on group membership, such as shared folders or databases.

Access control lists: Users can specify who is allowed to access a specific resource by creating a list of authorized users.

Mandatory Access Control (MAC):

Mandatory access control (MAC) is a type of access control where access to resources is determined by a central authority, and users do not have control over who is granted access.

Examples of MAC include:

Military clearance levels: Access to classified information is determined by the user's security clearance level.

Government agencies: Access to sensitive information is restricted to authorized personnel within a specific government agency.

Healthcare organizations: Access to patient medical records is restricted to authorized healthcare providers who require access to provide care.

Role-Based Access Control (RBAC):

Role-based access control (RBAC) is a type of access control where access to resources is based on the user's role or job function within the organization.

Examples of RBAC include:

Employee roles: Different employee roles have different levels of access to resources based on their job function, such as managers, executives, or customer service representatives.

User groups: Users can be grouped together based on their job function or department, and access to resources can be granted based on group membership.

Privilege levels: Users can be granted different levels of access to resources based on their role or job function, such as read-only access, edit access, or admin access.

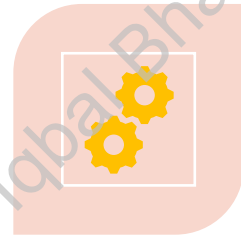
Access Control Implementation:



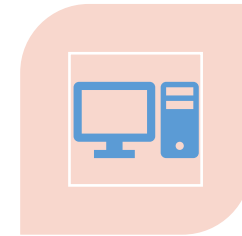
DEFINE ACCESS
CONTROL POLICIES



DEVELOP AN ACCESS
CONTROL PLAN



IMPLEMENT ACCESS
CONTROL
MECHANISMS



MONITOR ACCESS
CONTROL
MECHANISMS



MAINTAIN ACCESS
CONTROL
MECHANISMS

Prof. M. Iqbal Bhat (JKHED)

Questions?

