Security in Operating system

BY:

ROSHAN R. ROHIT

LECTURER,

IT DEPT,

GPG,SURAT

What is Operating System Security?

- The process of ensuring OS **availability, confidentiality, integrity** is known as operating system security.
- OS security refers to the processes or measures taken to protect the operating system from dangers, including viruses, worms, malware, and remote hacker intrusions.
- Operating system security comprises all preventive-control procedures that protect any system assets that could be stolen, modified, or deleted if OS security is breached.

The goal of Security System

Integrity

Unauthorized users must not be allowed to access the system's objects, and users with insufficient rights should not modify the system's critical files and resources.

Secrecy

The system's objects must only be available to a small number of authorized users. The system files should not be accessible to everyone.

The goal of Security System

Availability

All system resources must be accessible to all authorized users. If such a situation arises, service denial may occur.

In this case, malware may restrict system resources and preventing legitimate processes from accessing them.

Program threats

The operating system's processes and kernel carry out the specified task as directed. Program Threats occur when a user program causes these processes to do malicious operations.

The common example of a program threat is that when a program is installed on a computer, it could store and transfer user credentials to a hacker.

Virus

A virus may replicate itself on the system. Viruses are extremely dangerous and can modify/delete user files as well as crash computers.

A virus is a little piece of code that is implemented on the system program.

As the user interacts with the program, the virus becomes embedded in other files and programs, potentially rendering the system inoperable.

Trojan Horse

This type of application captures user login credentials.

It stores them to transfer them to a malicious user who can then log in to the computer and access system resources.

Logic Bomb

A logic bomb is a situation in which software only misbehaves when criteria are met; otherwise, it functions normally.

Trap Door

A trap door is when a program that is supposed to work as expected has a security weakness in its code that allows it to do illegal actions without the user's knowledge.

System threats

System threats are described as the misuse of system services and network connections to cause user problems.

These threats may be used to trigger the program threats over an entire network, known as program attacks.

System threats make an environment in which OS resources and user files may be misused.

Port Scanning

It is a method by which the cracker determines the system's vulnerabilities for an attack.

It is a fully automated process that includes connecting to a specific port via TCP/IP.

To protect the attacker's identity, port scanning attacks are launched through Zombie Systems, which previously independent systems now serve their owners while being utilized for such terrible purposes.

Worm

The worm is a process that can choke a system's performance by exhausting all system resources.

A Worm process makes several clones, each consuming system resources and preventing all other processes from getting essential resources.

Worm processes can even bring a network to a halt.

Denial of Service

Denial of service attacks usually prevents users from legitimately using the system.

For example, if a denial-of-service attack is executed against the browser's content settings, a user may be unable to access the internet.

HAVE ANY
QUERY

Security Measures and Policies in Operating System

BY:

ROSHAN R. ROHIT

LECTURER,

IT DEPT,

GPG,SURAT

Security Measures in Operating System

OS Security refers to practices and measures that ensure the confidentiality, integrity and availability of operating systems.

OS Security protects the system from various program threats like viruses,
Trojan horses, logic bombs, trap doors, ransomware and
system threats like port scanning, worms and denial of service attacks.

Security Measures

- Authentication
- Authorization
- Antivirus and malware protection
- Data backup
- Encrypted Data Transfer
- Firewalls
- Suspicious Emails and Links
- Use of Secure Wi-Fi only
- Personal Information Safeguards

OS Security Policies and Procedures

- Policy determines what should be done whereas Procedure determines how it is to be done.
- A security policy is a document that specifies the procedures used by an organization to ensure the confidentiality, integrity and availability of the system.
- Different organizations can have different policies based on the technologies they choose to work with.

Importance of Security Policy

A security policy provides guidance to implement access rights regarding which privileges to be granted to which users.

A security policy provides guidance regarding sharing of resources of an organization.

A security policy is helpful to meet regulatory and compliance requirements.

A security policy also improves organizational efficiency.

Examples of Common Security Policies & Procedures

Acceptable Use Policy(AUP): It defines the conditions and constraints under which a user can use an organization's resources.

Access Control Policy(ACP): It defines the access rights or privileges for users to access resources such as data and information of an organization.

Data/Information Security Policy: It defines data classification, ownership, encryption principles and data backup methodologies for the organization.

Examples of Common Security Policies & Procedures

Remote Access Policy: It defines methods of remotely connecting to an organization's network and accessing resources,

Firewall Policy: It describes the types of traffic an organization's firewall should allow/restrict.

Antivirus Policy: It describes installing and updating specific antivirus software into the computer systems.

Email/Communication Policy: It defines the rules or guidelines to communicate within the organization using organization-specific email domains or some other applications.

WHERE?
WHEN?
WHY?
WHAT? How? WHY?
WHERE?
How? WHO?
WHO?
WHAT?
WHERE?
WHEN?
How?
WHERE?
WHICH?
How?
WHEN? WHERE?
How?
WHAT? How? WHY?
WHY? How?
WHAT? How? WHY?
WHO? WHERE? WHAT? How?
WHAT?
WHY? How? WHERE?
WHO? WHOSE?
WHAT?
WHY?
WHO?
How?
WHERE? WHICH? WHOSE? WHAT WHY?
WHERE?
How?
How? WHO?
WHO? WHERE? WHAT? How?
WHAT? How? WHY?
WHERE?
How?
How?

User Authentication

BY:

ROSHAN R. ROHIT

LECTURER,

IT DEPT,

GPG,SURAT

User Authentication

It is the process of verifying the identity of a user that requests access to a system, network or a device.

User privileges depend upon the user's identity.

Based on the user identification, the OS can apply various authorizations like who can view which data and who can modify which data.

Authentication v/s Authorization

Authentication is process of verifying an identity of a user. User is required to produce evidence like a password for verification.

Authorization defines what the authenticated user is allowed to do or access.

It consists of two steps, where in the first step a user is granted privileges and in the second step, user's access rights are verified when a user needs to access a file.

Passwords

It is the most common method of user authentication.

Passwords can be in the form of a string of letters, digits, or special characters.

Users need to provide a username and password to authenticate themselves.

If the username and password match with those stored in the system, the user is considered as authentic user.

Password Vulnerabilities

GUESS

SHOULDER SURFING

PACKET SNIFFING

WRITTEN PASSWORDS

SHARING

One-Time Passwords(OTPs)

Along with standard authentication, one-time passwords give an extra layer of security.

Every time a user attempts to log into the One-Time Password system, a unique password is needed.

Once a one-time password has been used, it cannot be reused.

Secret Key

The user is given a hardware device that can generate a secret id that is linked to the user's id.

The system prompts for such a secret id, which must be generated each time you log in.

Random numbers

Users are given cards that have alphabets and numbers printed on them.

The system requests numbers that correspond to a few alphabets chosen at random.

Network Password

- Some commercial applications issue one-time passwords to registered mobile/email addresses, which must be input before logging in.

Authentication using Physical Object

To login into the system, the user must punch a card into a card slot or enter a key produced by a key generator into an option provided by the operating system.

Example: Usage of debit card at Automated Teller Machine(ATM).

Biometrics

- These techniques usually include biometric verification, such as fingerprints, retina scans, voice or speech, etc.
- This authentication is based on user uniqueness and is compared to database samples already in the system.
- Users can only allow access if there is a match.

Protection in Operating System

BY:

ROSHAN R. ROHIT

LECTURER,

IT DEPT,

GPG,SURAT

What is Protection in Operating System?

A mechanism that controls the access of programs, processes, or users to the resources defined by a computer system is referred to as protection.

You may utilize protection as a tool for multi-programming operating systems, allowing multiple users to safely share a common logical namespace, including a directory or files.

Need of Protection in Operating System

- There may be security risks like unauthorized reading, writing, modification, or preventing the system from working effectively for authorized users.
- It helps to ensure data security, process security, and program security against unauthorized user access or program access.
- It is important to ensure no access rights' breaches, no viruses, no unauthorized access to the existing data.
- Its purpose is to ensure that only the systems' policies access programs, resources, and data.

Goals of Protection in Operating System

The policies define how processes access the computer system's resources, such as the CPU, memory, software, and even the operating system. It is the responsibility of both the operating system designer and the app programmer.

Protection is a technique for protecting data and processes from harmful or intentional infiltration which contains protection policies either established by itself, set by management or imposed individually by programmers to ensure that their programs are protected to the greatest extent possible.

It also provides a multiprogramming OS with the security that its users expect when sharing common space such as files or directories.

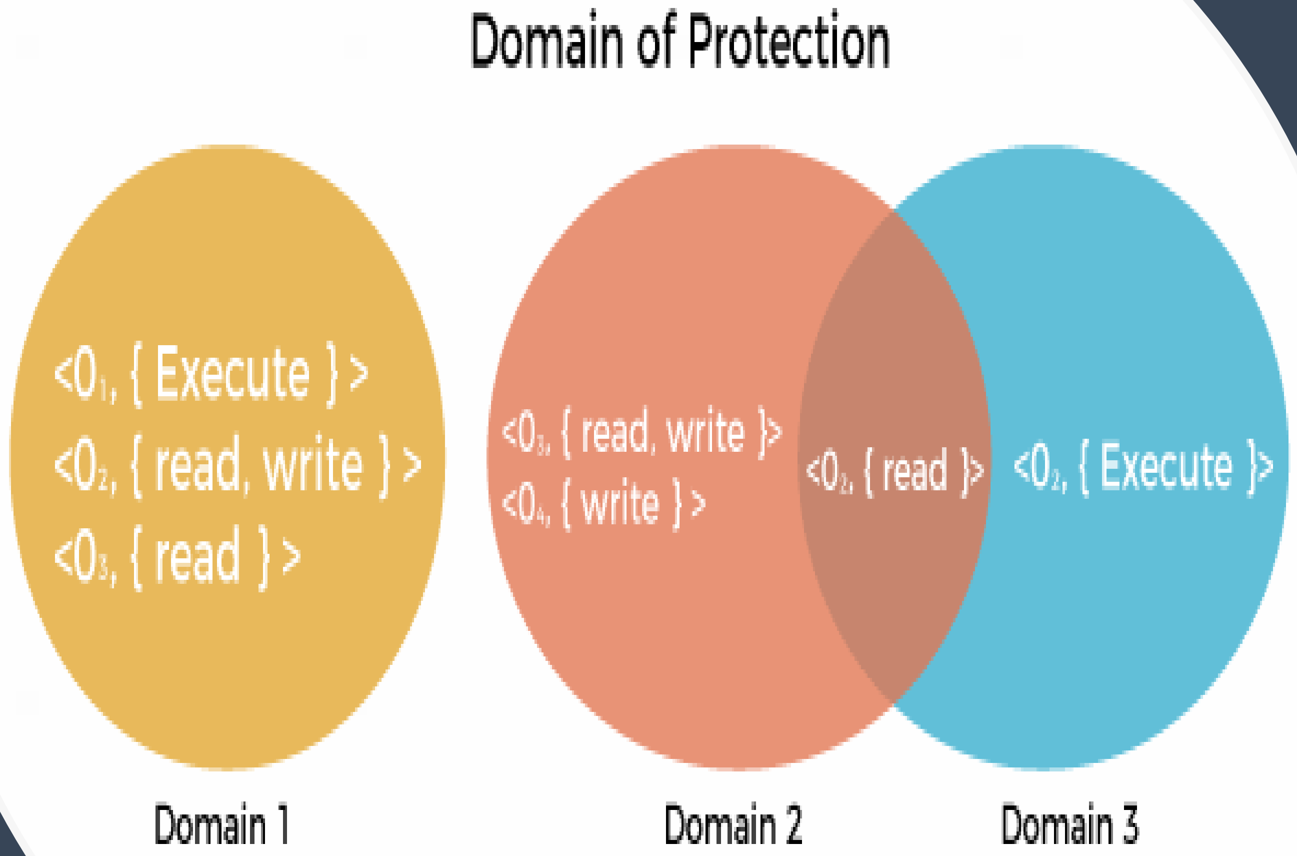
Protection Domain

The protection policies restrict each process's access to its resource handling.

A process is obligated to use only the resources necessary to fulfil its task within the time constraints and in the mode in which it is required. It is a process's protected domain.

Protection Domain

- Processes and objects are abstract data types in a computer system, and these objects have operations that are unique to them. A domain component is defined as **<object, {set of operations on object}>**.



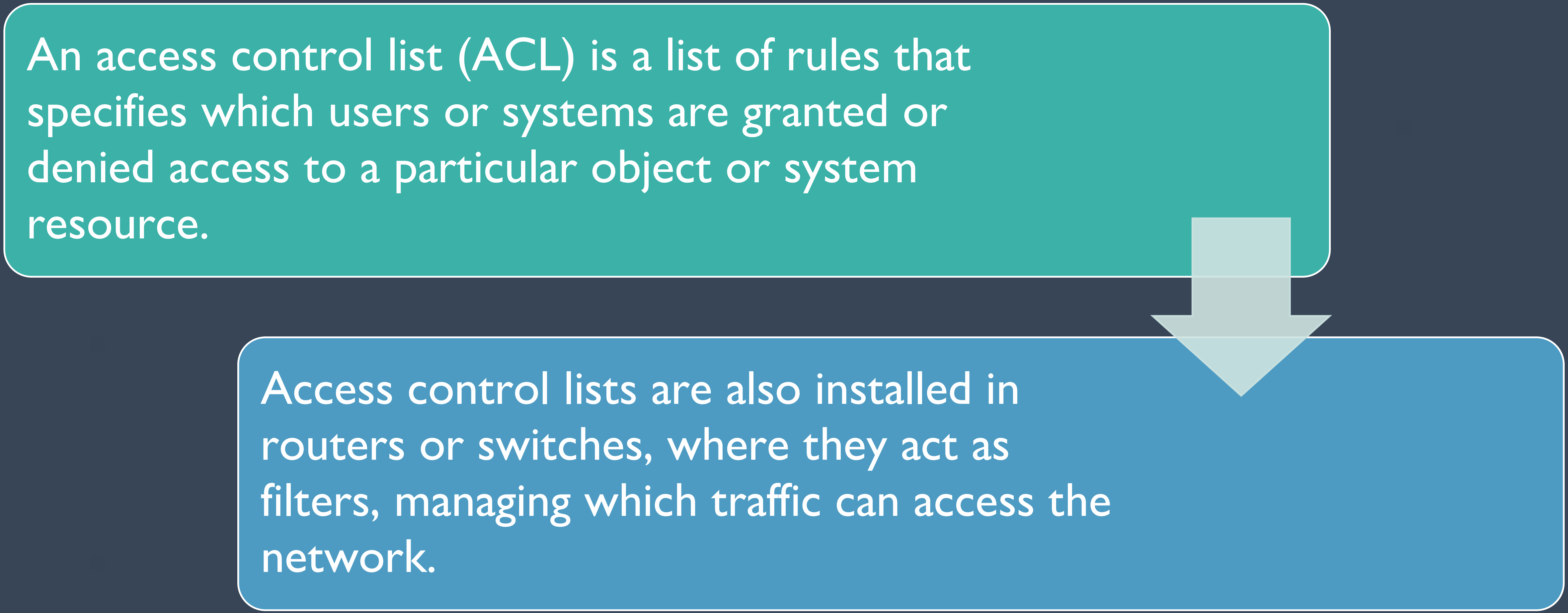
Protection Domain

Each domain comprises a collection of objects and the operations that may be implemented on them.

A domain could be made up of only one process, procedure, or user. If a domain is linked with a procedure, changing the domain would mean changing the procedure ID.

Objects may share one or more common operations.

Access Control List

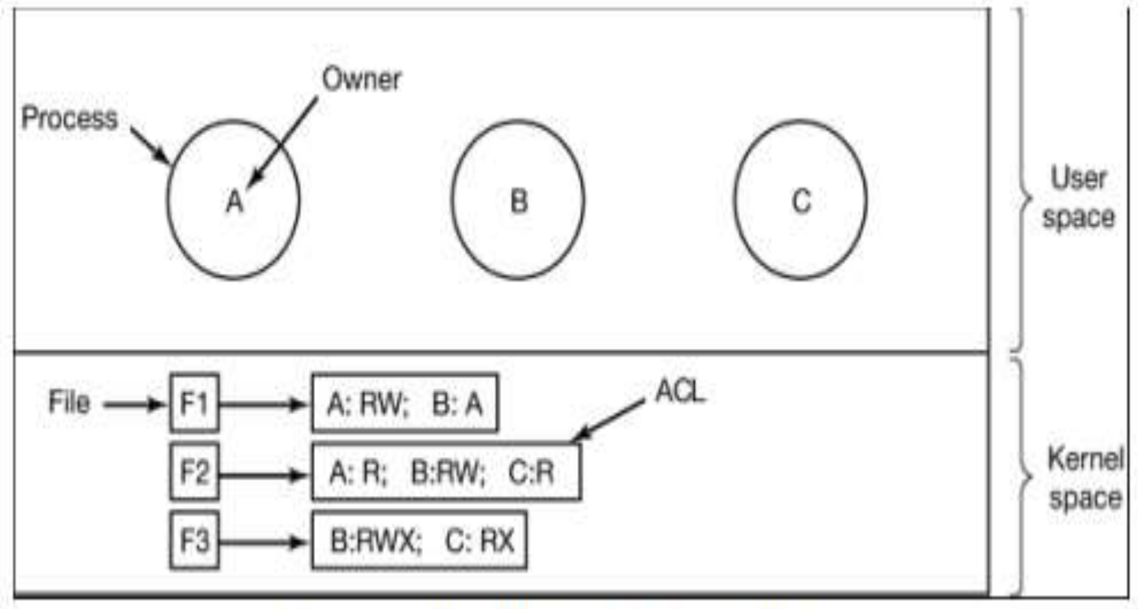


An access control list (ACL) is a list of rules that specifies which users or systems are granted or denied access to a particular object or system resource.

Access control lists are also installed in routers or switches, where they act as filters, managing which traffic can access the network.

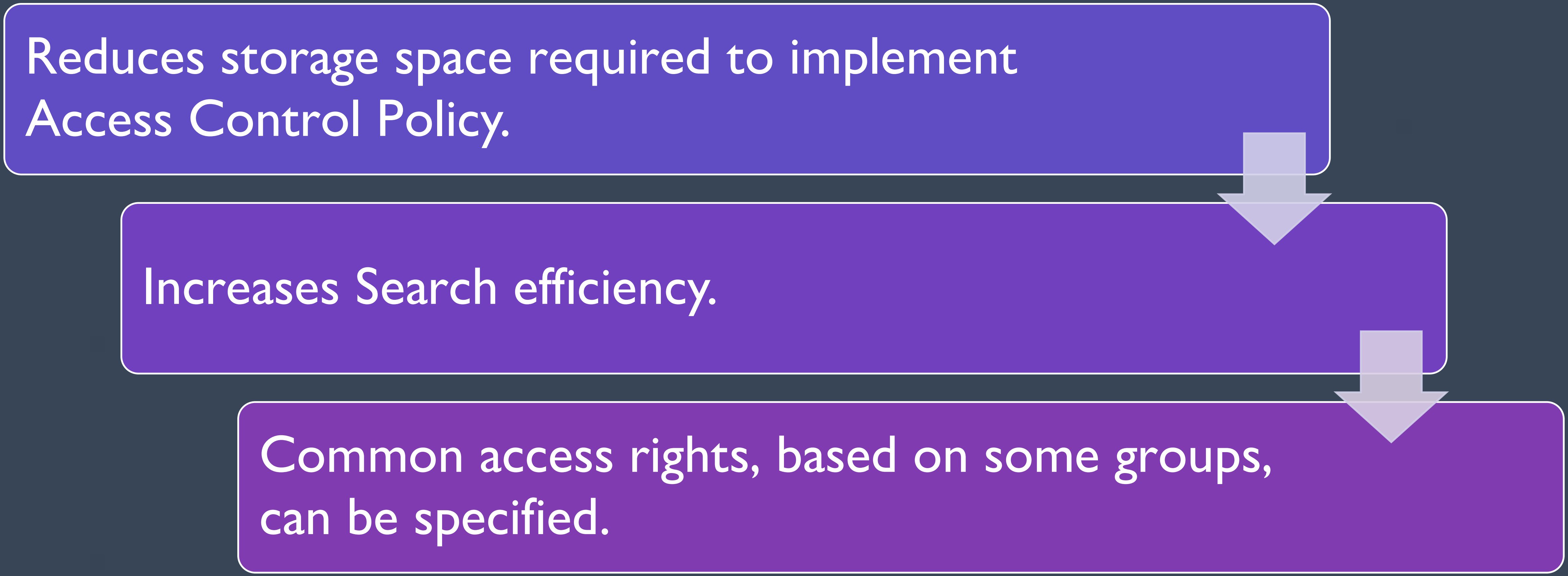
Access Control List (Example)

- ACLs work by creating tables that inform the operating system of access privileges given for certain system subjects.
- Each object has a unique security property that acts as an identification factor in its access control list.
- Some privileges include read/write privileges, file execution, and several others.



Use of access control lists to manage file access.

Access Control List (Advantages)



Reduces storage space required to implement Access Control Policy.

Increases Search efficiency.

Common access rights, based on some groups, can be specified.