

# Access Control: Implementation and Best Practices



By

Dr. Nawfal Fadhel

Contributors

Dr. Gary Wills

Dr. Faderica Paci

# Question

What is *Access*?

What is *Control*?

# What is Access Control

It is to give a trusted  
entity  
permission to access  
resource at  
some point in time.

It is to authenticate an  
entity,  
authorize it to access a  
resource and  
account for every action

# Question

Why is access control important?

# Importance of Access Control

## **Locally**

- It is used to differentiate inside users from outside users.
- help users to operate on their own personal data.

## **Network**

- It is used to give wide access to data and service.
- It holds all internet based services.
- Access control is achieved through means of (Access based defined) policies.

# Question

What are polices?

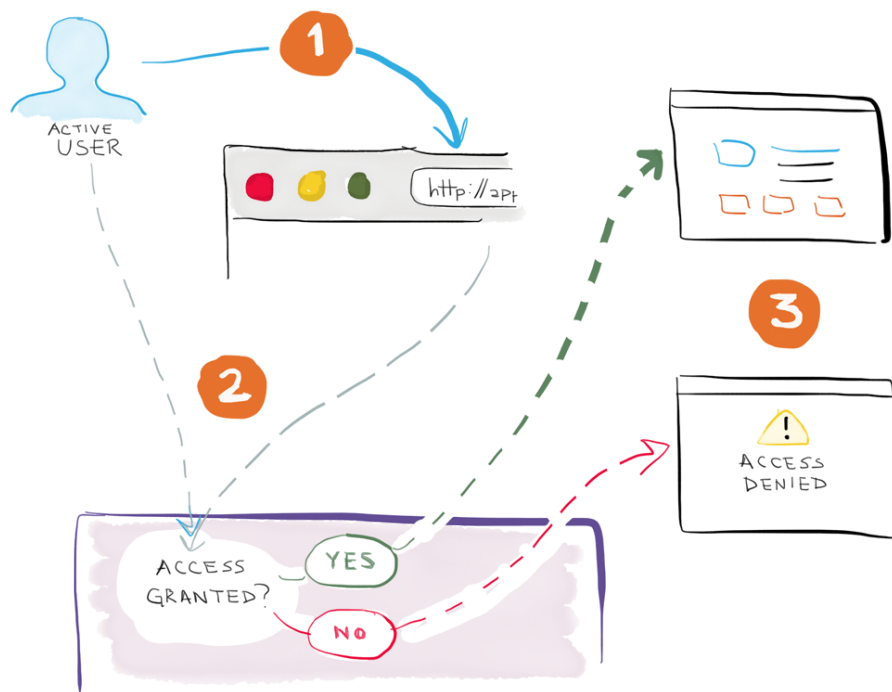
# Policy

Give X, permission to do Y within these  
constraints (such as time).

Examples:

# Web Access Control

- Web applications consist of elements that have different granularity levels and that are scattered through the entire application code.
- We need access control model and mechanism to deal with the distributed fine-grained access control code that protects the Web applications' elements.





# Web Access Control

- I. Database-oriented techniques where all access control is delegated to the database (eg. such as query rewriting to ensure people get only what they are entitled to see)
- II. Code-based approach that integrates the access control into the application code that is deployed on the server.

# Examples





## Database-oriented techniques

## Code-based approach






### Sharing settings

Link to share


<https://drive.google.com/drive/folders/1ehTwOFR5c0-WaiVIOxQzseg5M1Z9aqW?usp=sharing>

Share link via:    

Who has access

	Anyone who has the link can view	<a href="#">Change...</a>
	Bojan Siljanovski (you) bojan.s@gmail.com	is owner
	<div>help@coffeewithit.com</div>	 

Invite people:



Owner settings [Learn more](#)

☐ Prevent editors from changing access and adding new people

```
<?php
Class Acl {
    private $db;
    private $user_empty = false;

    //initialize the database object here
    function __construct() {
        $this->db = new db;
    }

    function check($permission,$userid,$group_id) {

        //we check the user permissions first
        If(!$this->user_permissions($permission,$userid)) {
            return false;
        }

        if(!$this->group_permissions($permission,$group_id) & $this->IsUserEm
            return false;
        }

        return true;
    }

    function user_permissions($permission,$userid) {
        $this->db->q("SELECT COUNT(*) AS count FROM user_permissions WHERE permis:
        $f = $this->db->f();

        If($f['count']>0) {
            $this->db->q("SELECT * FROM user_permissions WHERE permission_name='$per
            $f = $this->db->f();

            If($f['permission_type']==0) {
                return false;
            }

            return true;
        }
        $this->setUserEmpty('true');

        return true;
    }
}
```

# Importance of Access Control Design

- I. Access control models are used to:
  - I. Define a specific set of authorization rights.
  - II. Define a set of policies for a software system to enforce a set of rights to fulfil the security concerns.
  - III. Define a set of run-time system users that are used to assign the defined rights to the other users in the system.
  - IV. Protect for all multi-user systems, against violation of:
    - Confidentiality (eg. unauthorized disclosure)
    - Integrity (eg. improper modifications),
    - Availability (eg. Service disruption)

*Access control mechanism is the actual implementation of the access control model in the system.*

# Access Control Models

The main models of access control

- I. Discretionary (DAC)
- II. Mandatory (MAC).
- III. Role-based access control (RBAC) and its many flavours.

# Question

What dose the word Discretionary mean?

What dose the word Mandatory mean?

What dose the word Role based mean?

# What is the difference

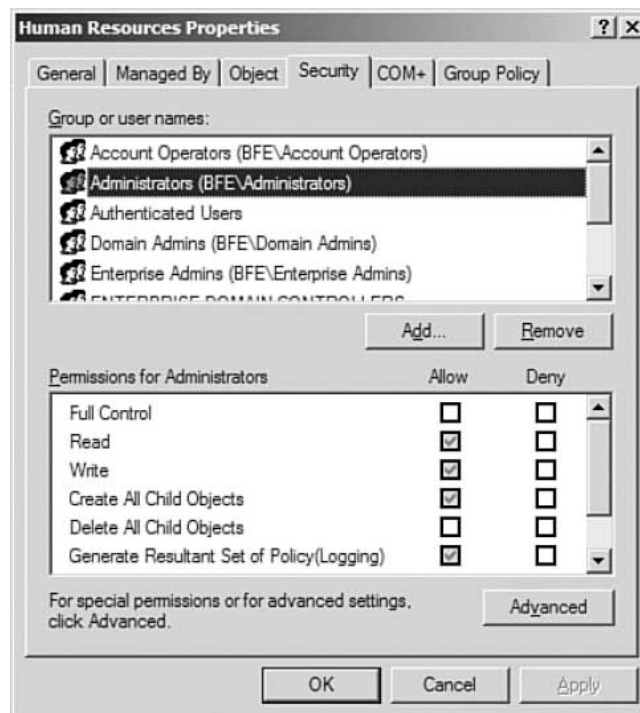
Discretionary is define by user.

Mandatory is define by a system.

Role Bases is define according to roles.

# Discretionary Access Control

- Probably the one you have come across the most.
  - Person want to perform an action on some data.
  - The access policy is consulted that check that that person has the access right to preform that operation.
  - Originated in operating systems
  - is often represented by the use of a matrix



The screenshot shows the 'File1: Permissions' dialog box. It displays a table with permissions for 'Owner', 'Group', and 'Others'. The permissions are 'Read', 'Write', and 'Execute'. The 'Owner' has all three permissions checked. The 'Group' has 'Read' and 'Execute' checked, but 'Write' is unchecked. The 'Others' have 'Read' and 'Execute' checked, but 'Write' is unchecked. At the bottom, the Octal permission is shown as '755' and the Text permission as 'rwxr-xr-x'.

	Read	Write	Execute
Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Others	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Octal: 755      Text: rwxr-xr-x

# Discretionary Access Control Issues

- As the access matrix represents the explicit access relation between each individual subject and object, it grows very large very quickly,
  - but remains sparse as most subjects remain unrelated to
  - This also leads to a complex authorization management.
  - The main drawback is that they are unable to enforce any sort of control of the flow of information from the process that is operating on behalf of the user .
  - This allows "Trojan Horse" processes to leak information



# Discretionary Access Control

- In the DAC context it is assumed that every object has an owner that controls the permissions to access the object.
- Owners have the ability to make policy decisions and/or assign security attributes.
- A straightforward example is the Unix file mode
  - Chmod 777 or Chmod 775

	Owner	Group	Everyone
0 – no permission	0	0	0
1 – execute	1	1	1
2 – write	2	2	2
3 – write and execute	3	3	3
4 – read	4	4	4
5 – read and execute	5	5	5
6 – read and write	6	6	6
7 – read, write, and execute	7	7	7

# Discretionary Access Control

- Chmod John Video\_folder 777
- Example
  - John wants her friend Alice to have view access on her photo album folder”Spanish Holidays”
  - John wants to share only with his wife his note.txt  
”Happy like the first day! Happy Anniversary my love!”
  - John wants to share with all his friends a funny video of her cat

	Owner	Group	Everyone
0 – no permission	0	0	0
1 – execute	1	1	1
2 – write	2	2	2
3 – write and execute	3	3	3
4 – read	4	4	4
5 – read and execute	5	5	5
6 – read and write	6	6	6
7 – read, write, and execute	7	7	7

# DAC Limitations

- Managing a policy is a complex task in a large system
  - Set of subjects or objects is large
  - Set of subjects or objects change frequently
- Capability Lists
  - Difficult to get an overview of permissions granted on a given object
- Access Control Lists
  - Difficult to get an overview of permissions granted to a given user

# Mandatory Access Control

- The most widely used MAC policy is the multi-level security policy model.
  - A process on behalf of the user, tries to access the object (note the user cannot access directly)
  - Allow MAC to also control indirect access from executed processes.
- There are four levels to multilevel security
  - I. Top Secret
  - II. Secret
  - III. Confidential
  - IV. Unclassified

# Mandatory Access Control

- MAC is a security strategy that restricts the ability individual resource owners have to grant or deny access to resource objects in a file system
  - Owners (users) cannot change these permissions.
- The policy are enforced by the operating systems or security kernel.

# Mandatory Access Control

- A security policy model is a succinct statement of the protection properties which a system, or generic type of system, must have.
  - Example: IoT, Blockchain, Cloudbased system
- Security policy is a document that expresses clearly and concisely what the protection mechanisms are to achieve.
- Typically it says: which user may access which data.
  - Example: DoomCorp Security policy
    1. Data shall be available only to those with ‘need to know’
    2. Anyone who breaches this policy shall be shot!!

# Mandatory Access Control

- When an entity attempts to access a specific resource, the OS or security kernel will check the entity's credentials to determine whether access will be granted.
- MAC requires careful planning and continuous monitoring to keep all resource objects' and users' *classifications* up to date.