Practical Application of DAC and RBAC on Windows 11

Dr. Brahim Ferik

Introduction

In this practical guide, we will explore how to implement **Discretionary Access Control (DAC)** and **Role-Based Access Control (RBAC)** on Windows 11. These access control models are essential for securing system resources and ensuring that only authorized users can access sensitive data.

Discretionary Access Control (DAC)

What is DAC?

- DAC allows users or administrators to define who can access specific resources.
- Users can set permissions on their own files and folders.

Applying DAC on Windows 11

Managing File and Folder Permissions

1. Open the file or folder you want to manage.
2. Right-click on it and select **Properties**.
3. Go to the **Security** tab.
4. Click **Edit** to modify permissions.
5. Add or modify user permissions (e.g., Full Control, Read, Write).

Example: Securing a Sensitive File

- Create a file named **secret.txt**.
- Set permissions so that only the user **Admin** has access:
  - Add **Admin** and grant **Full Control**.
  - Deny all other users access.

Using Command Prompt for DAC

Use the **icacls** command to manage file and folder permissions. Example:

```
icacls document.txt /grant user_test:R
```

This command grants the user **user__test** read-only access to **document.txt**.

Role-Based Access Control (RBAC)

What is RBAC?

- RBAC assigns permissions based on roles within an organization.
- Instead of setting permissions for individual users, permissions are assigned to roles, and users are added to these roles.

Applying RBAC on Windows 11

Creating Roles and Assigning Permissions

1. Open **Computer Management**:

   ```
   Win + R : lusrmgr.msc
   ```

2. Navigate to **Local Users and Groups > Groups**.
3. Right-click on **Groups** and select **New Group**.
4. Name the group (e.g., **Accounting**).
5. Add users to the group:
   - Right-click on the group and select **Add to Group**.
   - Add relevant users.

Assigning Permissions to the Role

1. Open the file or folder you want to secure.
2. Right-click and select **Properties**.
3. Go to the **Security** tab.
4. Add the group (e.g., **Accounting**) and assign appropriate permissions (e.g., Read, Write).

Example: Securing Financial Reports for the Accounting Department

- Create a group named **Accounting**.
- Add users from the accounting department to the group.
- Grant the **Accounting** group **Read** and **Write** permissions on the **Financial Reports** folder.

Practical Activities

Activity 1: Applying DAC to a Confidential File

1. Create a new file named **confidential.docx**.
2. Set permissions so that only the user **Admin** can read it.
3. Log in as another user and verify that they cannot access the file.

Activity 2: Applying RBAC to the Accounting Department

1. Create a group named **Accounting**.
2. Add users **user1** and **user2** to the group.
3. Grant the **Accounting** group **Read** and **Write** permissions on the **Financial Reports** folder.
4. Verify that members of the group can access the folder while others cannot.

Conclusion

- **Discretionary Access Control (DAC)** allows users to define permissions on their own resources.
- **Role-Based Access Control (RBAC)** is ideal for large organizations where roles simplify permission management.
- Both models can be applied effectively on Windows 11 using tools like **lusrmgr.msc**, **secpol.msc**, and command-line utilities such as **icacls**.