

The background of the slide is a dense, 3D-rendered field of numbers. The numbers are in various shades of blue and white, creating a sense of depth and movement. They are scattered across the entire frame, with some numbers appearing larger and more prominent than others. The overall effect is a complex, abstract pattern of digits.

Discretionary
Access
Control

What is DAC?



Access Control to Objects

Prevent
Determine
Grant
Revoke
Audit



Access control Components

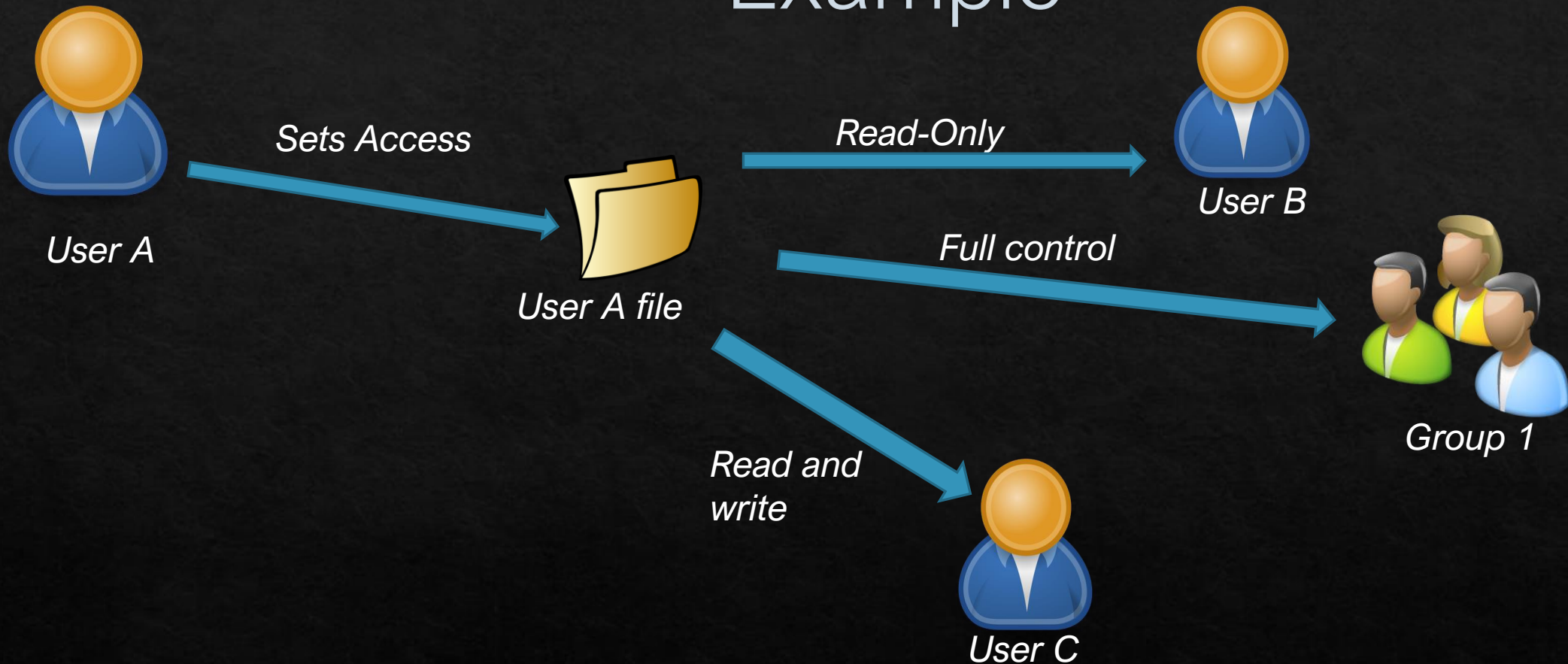
User
Subject
Object



Defined by each User

Access Control List
Groups
Users

Example



User A may provide read-only access on one of her files to User B, read and write access on the same file to User C and full control to any user belonging to Group 1.

Pros

- Grouping Employees together
- Customizable and Granular
- Flexible – user defined
- User Friendly

Cons

- Low Level of data protection
- Obscure, no centralized access management

Processes for assigning access

- Linux - chmod
 - r The read permission
 - w The write permission
 - x The execute permission
- Windows - Access Control Lists (ACL)
 - (Alice: read,write; bob: read)

```
mark@Marks-Lenovo:~$ ls -lq
total 0
drwxrwxrwx 1 mark mark 512 Jul 29 10:12 bin
-rw-rw-rw- 1 mark mark  0 Aug 20 10:35 example.txt
drwxrwxr-x 1 mark mark 512 Jul 20 13:03 gems
drwxrwxrwx 1 mark mark 512 Jul 18 14:10 lib
drwxrwxrwx 1 mark mark 512 Jul 18 14:10 share
mark@Marks-Lenovo:~$
```


Lifecycle of Account

- Based on the lifecycle of the account
- Administered by the individual file owners

Cross over

| | |
|---|---|
| <p>Mandatory Access Control (MAC):</p> <ul style="list-style-type: none">• Only system owner manages access control.• End user has no control over any privileges. | <p>Based Access Control (RBAC):</p> <ul style="list-style-type: none">• Provides access based on the position an individual has in an organization. |
| <p>Discretionary Access Control (DAC):</p> <ul style="list-style-type: none">• Least restrictive model.• Allows an individual complete control over any objects they own. | <p>Rule Based Access Control (RBAC).</p> <ul style="list-style-type: none">• Dynamically assign roles to users based on criteria defined by owner or system administrator. |