**13 B) Explain in detail the Access Control Mechanisms that can be employed in securing the information.**

In an operating system, access control lists are created by dividing the resource access matrix column-wise, whereas a capability list is created by dividing the access matrix row-wise. In this article, we will go through the access control list, and capability list, their advantage, and shortcomings along with the difference between the Access control list and the capability list.

## **Access Control List:**

Access Control lists can be created by splitting the access matrix column-wise. Access Control List is the object-wise list that specifies the list of subjects that have access to a particular object along with their access right. In simple terms, the ACL. of an object defines the list of users and the operations that they can perform on that object. Each object has a security attribute that identifies its access control list. A filesystem Access Control list is a data structure containing entries that specify an individual user or group’s rights to specific system objects such as programs, processes, or files. These entries are known as **access-control entries.**

### **Advantages of Access Control List:**

* It is easy to change by removing the entry of the subject from the object’s access control list.
* It is easy to review access by directly examining the access control list of objects.

### **Disadvantages of Access Control List:**

* It imposes search overhead and results in poor efficiency as the entire access control list needs to be searched when access is made to an object.
* It requires more data storage space as data is stored object-wise and the same subject can have multiple access to multiple objects thereby consuming more storage space.

## **Capability Lists:**

Capability lists can be created by splitting the access matrix row-wise. A capability list is a subject-wise list that specifies the list of rights the subject has for every object. Thus, the capability list of a user or a process or domain is a list of rights that it has on the various objects. A capability consists of two fields-object descriptor access rights. An object descriptor is an identifier for an object and access right indicates various operations such as read, write execute, etc. granted to an object. A capability can be given as a pair (x, r) where **x** is the name of an object and **r** is a set of privileges or rights.

### **Advantages of Capability List:**

* It is efficient as it frequently checks the validity of an address.
* It is flexible as users are allowed to define certain parameters.
* It is simple to understand as it allows natural correspondence between subjects and objects.

### **Limitations of Capability Lists:**

* It is difficult to deallocate memory that is not currently in use.
* It is difficult to change access rights once assigned to subjects.
* It has complicated control of the propagation of various access rights.
* It is difficult to review the access provided to various subjects.

### **Difference between the Access Control list and Capability list:**

| **Sr. No** | **Access Control Lists** | **Capability Lists** |
| --- | --- | --- |
| **1.** | It is defined object-wise (resources). | It is defined subject-wise (users, processes, and procedures). |
| **2.** | It lists the various subjects along with the rights of an object. | It lists the various objects along with the rights permitted on them for a subject. |
| **3.** | Each object (resource) has a list of pairs of the form <subject, access rights> | Each subject (user, process procedure) has a list of pairs of the form <object, access rights> |
| **4.** | It would be tedious to have separate listings for each object (user), therefore, they are grouped into classes. For example, in UNIX, there are three classes self, group, and anybody else. | Here capabilities are the names of the objects. The objects not referred to in at capability list cannot be ever named. |
| **5.** | The default is: Everyone should be able to access a file. | The default is: No one should be able to access a file unless they have been given a capability. |
| **6.** | Access lists are simple and are used in almost all file systems. | Capabilities are used in systems that need to be very secure as they prohibit sharing of information unless access is given to a subject. |