Book start

content *text*

Term

Definition 1

This is a definition.

Definition 2: Context

This is a definition.

> This is a quote.

Another Term

Definition 3

This is a definition.

Definition 4: Context

This is a definition.

> This is a quote.

Access Control List

Alternate Forms

Ackle `Prononciation` ACL `Acronym`

Definitions

Definition 5: Definition 1

A digital representation listing the principals that have access to a resource and the operations that they are authorized to execute on it.

It is used by the *reference monitor* to allow or deny access requests to the resource.

It is a *discretionary access control* mechanism, i.e. authorized users such as *resource owners* have the possibility to modify it, effectively granting and revoking access permissions.

It is linked to (and sometimes embedded in) the resource. This may be an advantage as it provides flexibility with an *access granularity level* set at the individual resource. This may be a disadvantage as managing ACLs at scale becomes inefficient, function of the number of *resources* , the number of *principals* and the *stability of access decision factors* .

It may be considered as resource metadata.

Related Terms

Access (Dictionary Entry) Access Control (Dictionary Entry) Access Granularity (Dictionary Entry) AWS ACL (Dictionary Entry) `Product-specific Implementation` Discretionary Access Control `Generic Form` Linux ACL Resource Stability of Access Decision Factors (Dictionary Entry) Windows ACL

Quotes

> Access Control List (ACL). The access matrix is implemented through a set of lists, one for each object (i.e., the columns of the matrix) in the system. The list associated with an object has an element for each subject holding a privilege on the object. This element contains the set of privileges the subject can exercise on the object. This is the way usually adopted by modern operating systems.

(Ferrari, 2010, p. 12)

(Ferrari, 2010 , p. 12)

> 4.2.2 Access Control ListsAnother way of simplifying the management of access rights is to store the access control matrix a column at a time, along with the resource to which the column refers. This is called an access control list or ACL (pronounced ‘ackle’). In the first of our above examples, the ACL

> for file 3 (the account file) might look as shown here in Figure 4.4.ACLs have a number of advantages and disadvantages as a means of managing security state. These can be divided into general properties of ACLs, and specific properties of particular implementations.ACLs are a natural choice in environments where users manage their own file security, and became widespread in the Unix systems common in universities and science labs from the 1970s. They are the basic access control mechanism in Unix-based systems such as GNU/Linux and Apple's OS/X; the access controls in Windows are also based on ACLs, but have become more complex over time. Where access control policy is set centrally, ACLs are suited to environments where protection is data-oriented; they are less suited where the user population is large and constantly changing, or where users want to be able to delegate their authority to run a particular program to another user for some set period of time. ACLs are simple to implement, but are not efficient as a means of doing security checking at runtime, as the typical operating system knows which user is running a particular program, rather than what files it has been authorized to access since it was invoked. The operating system must either check the ACL at each file access, or keep track of the active access rights in some other way.Finally, distributing the access rules into ACLs means that it can be tedious to find all the files to which a user has access. Revoking the access of an employee who has just been fired will usually have to be done by cancelling their password or other authentication mechanism. It may also be tedious to run system-wide checks; for example, verifying that no files have been left world-writable could involve checking ACLs on millions of user files.

(Anderson, 2008, p. 99)

(Anderson, 2008 , p. 99)

> Access control listA list of principals that are authorized to have access to some object.

(Saltzer and Schroeder, 1975, p. 1)

(Saltzer and Schroeder, 1975 , p. 1)

Bibliography

Saltzer and Schroeder, 1975

See Also

false 50 title label = "access-control-list"

Unanticipated User

Definitions

Definition 6: Definition 1

A user whose onboarding was not anticipated.

Unanticipated users may occur when the onboarding process is not established and followed, or when the circumstances that trigger the onboarding process are such that it couldn't be followed.

The absence of a process to manage the unanticipated users may have adverse effects on the organization. When the onboarding process is not established or followed, it is a managerial issue. When the onboarding process couldn't be followed, depending on requirements, self-registration, identity federation, ABAC, PBAC may help manage *unanticipated users* .

Related Terms

ABAC Entity (Dictionary Entry) Identity Federation Onboarding Process PBAC Unanticipated Entity `Generic Form` User (Dictionary Entry)

Quotes

> 3.3 Need to Support Unanticipated Users – The approach for establishing a requesters' identity may be driven by the need to support entities that were not necessarily expected to require such access. For example, in a military operation, there may be a need to expand the involvement of personnel from other agencies e.g., intelligence analysts who were not initially anticipated. If the identity approach selected uses DoD credentials, each analyst identified initially would be issued a DoD credential. In this scenario, each new analyst identified would need to be issued a DoD credential. This would mean that each new analyst has to physically visit a DoD Registration Authority. That operator has to validate that the user's registration is approved, establish the user's true identity, registered him in a DoD repository of authorized users, and create and issue the user a PKI certificate.The requester identity approach selected may be very appropriate for large user populations where users can be identified well in advance of their need for access. However, even if the approval, registration and issuance process could be expedited, the time required to register new personnel may have an adverse impact on the mission operation. It may be more effective to select an identification scheme that can recognize and authenticate identity credentials issued by other US federal agencies. Access control mechanisms such as ABAC and PBAC lend themselves to more sophisticated access control rules that can include

> provisions for allowing more flexible identification schemes

(Farroha and Farroha, 2012, p. 3)

(Farroha and Farroha, 2012 , p. 3)

Bibliography

Farroha and Farroha, 2012

See Also

false title label = "unanticipated-user"

Stability of Access Decision Factors

Definitions

Definition 7: Definition 1

The average period during which access decision factors are only subject to slight disturbance, prolonging the validity of previously defined access permissions. A disturbance of access decision factors beyond some threshold triggers the requirement to adapt access permissions. Distinct access control methods (e.g. ACL, RBAC, ABAC, PBAC) are varyingly efficient in the way they enable modifications of access permissions.

Related Terms

ABAC Access (Dictionary Entry) Access Control (Dictionary Entry) Access Control List (Dictionary Entry) PBAC RBAC

Quotes

> 3.1 Stability of Access Decision Factors – When the basis for access decisions is relatively stable, use of mechanisms such as ACLs lends itself more readily. Administrative processes typically required to maintain these lists are time-intensive and not particularly well suited to situations where significant changes and updates are required frequently. On the other hand, use of a flexible Attribute Management enterprise service where attributes can be easily managed, may be more responsive and thus, more operationally effective.

(Farroha and Farroha, 2012, p. 3)

(Farroha and Farroha, 2012 , p. 3)

Bibliography

Farroha and Farroha, 2012

See Also

false title label = ”stability-of-access-decision-factors”
Book end