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.

AWS IAM

Definitions

Definition 5: Definition 1AWS

The native IAM platform in AWS.

Related Terms

1. AWS
2. AWS Account
3. (link)
4. (link)
5. (link)
6. (link)
7. (link)
8. (link)

Quotes

> AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

(AWS, 11/2020, p. 1)
(Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html)

((link) , p. 1) (Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html)

Bibliography

1. (link)

See Also

label = ”aws-iam” false title

AWS IAM Policy

Definitions

Definition 6: Definition 1AWS

An access policy in AWS.

Related Terms

1. AWS
2. AWS Account
3. (link)
4. AWS IAM
5. (link)
6. (link)
7. (link)

Quotes

> Policies and Permissions in IAMYou manage access in AWS by creating policies and attaching them to IAM identities (users, groups of users, or roles) or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when an IAM principal (user or role) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. AWS supports six types of policies: identity-based policies, resource-based policies, permissions boundaries, Organizations SCPs, ACLs, and session policies.IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, if a policy allows the GetUser action, then a user with that policy can get user information from the AWS Management Console, the AWS CLI, or the AWS API. When you create an IAM user, you can choose to allow console or programmatic access. If console access is allowed, the IAM user can sign in to the console using a user name and password. Or if programmatic access is allowed, the user can use access keys to work with the CLI or API..

(AWS, 11/2020, p. 351)
(Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html)

((link) , p. 351) (Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html)

Bibliography

1. (link)

See Also

label = ”aws-iam-policy” false title

AWS IAM Temporary Security Credentials

Definitions

Definition 7: Definition 1AWS

A temporary identity in AWS.

Related Terms

1. AWS
2. AWS Account
3. (link)
4. AWS IAM
5. (link)
6. (link)
7. (link)

Quotes

> Temporary security credentials in IAMYou can use the AWS Security Token Service (AWS STS) to create and provide trusted users with temporary security credentials that can control access to your AWS resources. Temporary security credentials work almost identically to the long-term access key credentials that your IAM users can use, with the following differences: • Temporary security credentials are short-term, as the name implies. They can be configured to last for anywhere from a few minutes to several hours. After the credentials expire, AWS no longer recognizes them or allows any kind of access from API requests made with them. • Temporary security credentials are not stored with the user but are generated dynamically and provided to the user when requested. When (or even before) the temporary security credentials expire, the user can request new credentials, as long as the user requesting them still has permissions to do so.These differences lead to the following advantages for using temporary credentials: • You do not have to distribute or embed long-term AWS security credentials with an application. • You can provide access to your AWS resources to users without having to define an AWS identity for them. Temporary credentials are the basis for roles and identity federation. • The temporary security credentials have a limited lifetime, so you do not have to rotate them or explicitly revoke them when they're no longer needed. After temporary security credentials expire, they cannot be reused. You can specify how long the credentials are

> valid, up to a maximum limit.

(AWS, 11/2020, p. 301)
(Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html)

((link) , p. 301) (Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html)

Bibliography

1. (link)

See Also

label = ”aws-iam-temporary-security-credentials” false title

AWS IAM Group

Definitions

Definition 8: Definition 1AWS

A security group in AWS. It contains *AWS IAM Users* and may be granted permissions via policies. It has a flat structure, i.e. AWS IAM does not support group nesting.

Related Terms

1. ARN
2. AWS
3. AWS Account
4. AWS IAM
5. (link)
6. Group

Quotes

> IAM GroupsAn IAM group is a collection of IAM users. Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users. For example, you could have a group called Admins and give that group the types of permissions that administrators typically need. Any user in that group automatically has the permissions that are assigned to the group. If a new user joins your organization and needs administrator privileges, you can assign the appropriate permissions by adding the user to that group. Similarly, if a person changes jobs in your organization, instead of editing that user's permissions, you can remove him or her from the old groups and add him or her to the appropriate new groups.Note that a group is not truly an "identity" in IAM because it cannot be identified as a Principal in a permission policy. It is simply a way to attach policies to multiple users at one time.Following are some important characteristics of groups:- A group can contain many users, and a user can belong to multiple groups.- Groups can't be nested; they can contain only users, not other groups.- There's no default group that automatically includes all users in the AWS account. If you want to have a group like that, you need to create it and assign each new user to it.- The number and size of IAM resources in an AWS account are limited. For more information, see IAM and STS quotas.

(AWS, 11/2020, p. 160)
(Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html)

((link) , p. 160) (Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html
)

Bibliography

1. (link)

See Also

false title label = ”aws-iam-group”

AWS Account Root User

Definitions

Definition 9: Definition 1AWS

The root user of an AWS account, with unlimited privileges on the account and its resources.

Related Terms

1. AWS
2. Root User

Quotes

> AWS account root userWhen you first create an Amazon Web Services (AWS) account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account.

(AWS, 11/2020, p. 72)
(Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html)

((link) , p. 72) (Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html)

Bibliography

1. (link)

See Also

label = ”aws-account-root-user” false title

AWS ACL

Alternate Forms

1. AWS Access Control List

Definitions

Definition 10: Definition 1AWS

An ACL implementation specific to AWS whose scope is limited to granting access to identities outside the AWS Account that contains the resource. Contrary to other AWS policy types, AWS ACL is not following the AWS JSON policy format.

Related Terms

1. (link) `Generic Form`
2. AWS
3. AWS Account
4. AWS IAM
5. (link)

Quotes

> Access control lists (ACLs)Access control lists (ACLs) are service policies that allow you to control which principals in another account can access a resource. ACLs cannot be used to control access for a principal within the same account. ACLs are similar to resource-based policies, although they are the only policy type that does not use the JSON policy document format. Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs.

(AWS, 11/2020, p. 353)
(Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html)

((link) , p. 353) (Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html)

Bibliography

1. (link)

See Also

false title label in (”aws-access-control-list” , ”aws-acl”)

AWS IAM Role

Definitions

Definition 11: Definition 1AWS

A temporary on-demand business role in AWS. Once an identity is granted permission to assume a role, the identity may assume that role by demanding it. It then inherits all of the access permissions linked to it.

Related Terms

1. AWS
2. AWS Account
3. (link)
4. AWS IAM
5. (link)
6. (link)

Quotes

> IAM RolesAn IAM role is an IAM identity that you can create in your account that has specific permissions. An IAM role is similar to an IAM user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have standard longterm credentials such as a password or access keys associated with it. Instead, when you assume a role, it provides you with temporary security credentials for your role session.You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. For example, you might want to grant users in your AWS account access to resources they don't usually have, or grant users in one AWS account access to resources in another account. Or you might want to allow a mobile app to use AWS resources, but not want to embed AWS keys within the app (where they can be difficult to rotate and where users can potentially extract them). Sometimes you want to give AWS access to users who already have identities defined outside of AWS, such as in your corporate directory. Or, you might want to grant access to your account to third parties so that they can perform an audit on your resources.For these scenarios, you can delegate access to AWS resources using an IAM role.

(AWS, 11/2020, p. 167)
(Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html)

((link) , p. 167) (Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html
)

Bibliography

1. (link)

See Also

false title label = ”aws-iam-role”

AWS IAM User

Definitions

Definition 12: Definition 1AWS

An identity in AWS. It is mapped to either a person or an application. It has 3 identifiers: a friendly name, an ARN and a unique ID. It is linked to a single *AWS Account* . It may be a member of *AWS IAM Groups* . It may be granted direct permissions or indirect permissions via *AWS IAM Group* membership.

The *AWS Account Root User* is not considered as an *AWS IAM User* .

Related Terms

1. ARN
2. AWS
3. AWS Account
4. (link)
5. AWS IAM
6. (link)

Quotes

> IAM UserAn AWS Identity and Access Management (IAM) user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user in AWS consists of a name and credentials.

(AWS, 11/2020, p. 74)
(Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html)

((link) , p. 74) (Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html)

Bibliography

1. (link)

See Also

false title label = ”aws-iam-user”

Mutual Authentication

Definitions

Definition 13: Definition 1

A communication scheme where both communicating entities are authenticated to each other.

Mutual authentication requires more than two unilateral authentications in opposite directions, because of the relationship between these two opposite processes.

Mutual authentication protects against unauthorized access by mitigating man-in-the-middle attacks. In certain circumstances, it may mitigate DoS attacks as well.

When communication takes place between a server and a client, authentication of the client by the server may be incorrectly perceived as the only important security aspect. But without authentication of the server by the client, the server itself may be spoofed leading the way to multiple attacks.

Related Terms

1. (link)
2. Unilateral Authentication

Quotes

> SRP-8REQUIREMENT: The CSP SHALL ensure that all communications occur over a mutually authenticated protected channel. (5.3.3.2 #7)SUPPLEMENTAL GUIDANCE: Mutually authenticated protected channels employ approved cryptography to encrypt communications between (sic)Supervised remote identity proofing stations/kiosks are required to employ mutual authentication where both the station/kiosk and server authenticate to each other. This is most often accomplished through the use of mutual TLS. Upon successful mutual authentication, an encrypted communication channel is established between the workstation/kiosk and the server which protects the data exchanged between them.ASSESSMENT OBJECTIVE: Confirm the CSP's supervised remote identity proofing stations or kiosks communicate with the identity service via mutually authenticated protected channels.POTENTIAL ASSESSMENT METHODS AND OBJECTS: Examine: one or both the of the following: system documentation, such as remote identity proofing station specifications; or an actual supervised remote identity proofing station (kiosk) employed by the CSP.

(Fenton, 2020, p. 58-59)

((link) , p. 58-59)

> 3.2.2.4 Authentication and Data Integrity between ABAC ComponentsThe authorization service requires strong mutual authentication between ABAC components (e.g., PEP, PDP) when authorization service components exchange sensitive information. For each exchange, proof of origin, data integrity, and timeliness should be considered. For example, when the authorization service needs to obtain attributes from an authoritative attribute service, mutual authentication should be used, followed by mechanisms for validating message integrity and message origin. Authentication protocols based on strong methods (e.g., X.509 authentication) should be used to provide the level of assurance needed by both parties involved in the attribute exchange.

(NIST SP 800-162, 2014, p. 28)

((link) , p. 28)

> RADIUS(…)- Mutual authentication support: Man-in-the-middle attacks are possible with one-way authentication. Mutual authentication eliminates this risk by authenticating the RADIUS server and the client. The client initially passes its identification to the server, which responds with its identification so that both the server and the client are assured of mutual reliability. The same happens with the AP and the server.

(EC-Council, 2010, § 5-35)

((link) , § 5-35)

> DHCP Services(…)RFC 3118 appends authentication to DHCP and permits a client to confirm whether a specific DHCP server can be relied on and whether a request for DHCP information originates from a client that is certified to use the network. This mutual authentication in DHCP presents the additional security advantage of helping to protect DHCP clients and servers from DoS attacks and unauthorized access. RFC 3118 describes a method that can present both individual certification and message confirmation. This helps a DHCP client verify the uniqueness of the DHCP server it chooses in an unsecured network environment. This operation is very helpful for both a standard company Ethernet network and an Internet service provider (ISP).

(EC-Council, 2010, § 5-38-39)

((link) , § 5-38-39)

> 11.4.2 Mutual AuthenticationThe basic mechanisms for message freshness or principal-liveness introduced so far achieve so-called ”unilateral authentication” which means that only one of the two protocol participants is authenticated. In mutual authentication, both communicating entities are authenticated to each other.ISO and IEC have standardized a number of mechanisms for mutual authentication. A signature based mechanism named ”ISO Public Key Three-Pass Mutual Authentication Protocol” [148] is specified in prot 11.1. We choose to specify this mechanism in order to expose a common misunderstanding on mutual authentication.One might want to consider that mutual authentication is simply twice unilateral authentication; that is, mutual authentication could be achieved by applying one of the basic unilateral authentication protocols in §11.4.1 twice in the opposite directions. However, this is not generally true!A subtle relationship between mutual authentication and unilateral authentication was not clearly understood in an early stage of the ISO/IEC standardization process for prot 11.1. (…)

(Mao, 2003, § 11.4.2)

((link) , § 11.4.2)

> mutual authenticationAuthentication of both ends of a communication session.OverviewTraditional network authentication systems have centered around having the server authenticate the credentials of the client. They ignore authentication of the server by the client since it is assumed that the server is always a trusted entity. However, it is sometimes possible to spoof the identity of a server, especially in an Internet scenario in which information is sent over an insecure public communication system and is subject to eavesdropping, interception, and hijacking. Although simple consumer transactions such as users buying goods online may suffice with one-way authentication of clients by e-commerce servers, more costly business-to-business (B2B) and financial industry transactions need both ends of a communication channel to be authenticated before establishing a session and per- forming a transaction. Mutual authentication is the general term for any scheme by which both parties authenticate the other prior to sending sensitive information to each other.One protocol that was developed for mutual authentication is Kerberos, a popular authentication protocol developed by the Massachusetts Institute of Technology (MIT) and used by Active Directory directory service in Microsoft Windows 2000 and Windows Server 2003. Other mutual authentication protocols include the following: Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) Extensible Authentication Protocol/Transport Layer Security (EAP/TLS) Symmetric-Key Three-Pass Mutual Authentication Protocol defined in the ISO 9798 standardSee Also:

> authentication, Kerberos

(Tulloch, 2003, p. 199)

((link) , p. 199)

Bibliography

1. (link)
2. (link)
3. (link)
4. (link)
5. (link)

See Also

false title label = ”mutual-authentication”

Stability of Access Decision Factors

Definitions

Definition 14: 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

1. ABAC
2. (link)
3. (link)
4. (link)
5. PBAC
6. 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)

((link) , p. 3)

Bibliography

1. (link)

See Also

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

RA

e-Identity

RP

Registration Authority

Credential Service Provider

IAM Management

Control Party

Identity Provider

Access Control List

Alternate Forms

1. Ackle `Prononciation`
2. ACL `Acronym`

Definitions

Definition 15: 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

1. (link)
2. (link)
3. (link)
4. (link) `Product-specific Implementation`
5. Discretionary Access Control `Generic Form`
6. Linux ACL
7. Resource
8. (link)
9. 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)

((link) , 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)

((link) , p. 99)

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

(Saltzer and Schroeder, 1975, p. 1)

((link) , p. 1)

Bibliography

1. (link)

See Also

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

Authentication Factor

Strong Authentication

Broker

AP

Attribute Provider

IdP

Weak Authentication

4-Eyes Principle

Alternative Forms

1. 2-Person Control
2. 4-Eyes Check
3. Dual Authorization
4. Four-Eyes Check
5. Four-Eyes Principle
6. Two-Person Control

Definitions

Definition 16: Definition 1Audit, IAM, Access Management

A type of segregation of duties control which prescribes that crucial decisions or operations be prepared by one actor, and reviewed and validated by another actor before the decision or the operation becomes effective. This setup contrasts with decisions or operations that may be made by individual actors. This control mitigates the risk of inconsiderate, fraudulent or suboptimal decisions.

Related Terms

1. (link)

Quotes

> An instrument often used to reduce the risk of inconsiderate, fraudulent or suboptimal decisions in all types of organizations – and not just in family firms – is the four-eyes principle (4EP) (Sutter, 2007; Feldbauer-Durstmüller et al., 2012; Six et al., 2012; Bátiz-Lazo and Noguchi, 2013)[1]. This principle usually means that crucial decisions (often defined as those affecting a certain minimum amount of capital) may not be made by individual actors alone but must be jointly made by at least two actors. The inclusion of at least two actors also explains why the principle's name includes "four eyes". This approach ensures the rationality of decisions as well as reciprocal control of decisions (Schickora, 2010). This is why Gottschalk (2011, p. 300), based on a study of executives involved in white-collar crime, states that "the 4EP should always be applied" in management decisions. In addition, the 4EP not only mitigates high-risk decision outcomes but also enriches the decision-making process by integrating the views of different individuals (Knoll, 2013).

(Hiebl, 2015, p. 1-2)

((link) , p. 1-2)

Bibliography

1. (link)

See Also

false title label = "4-eyes-principle"

Single Login

Enterprise Single Sign-On

ESSO

Single Sign-On

SSO

Web-based Single Sign-On

Multidomain Single Sign-On

IT Asset Scope

Permission

Principal

Subject

Privilege

Object

Enterprise Identity Management

Deprovisioning

EIdM

Account

Alternative Forms

1. a/c `Abbreviation`
2. Acc. `Abbreviation`
3. Digital Account `more precise form`
4. Identity `Near Synonym`
5. User Account `Synonym`

Definitions

Definition 17: Definition 1

In the literature, *account* is generally used a synonym for *identity* .

Because the definition of *identity* is defined as a set of identifier, credential and other attributes linked to an *entity* , *account* could be used to distinguish technical and privileged accounts that are not necessarily linked to an entity, from *identities* or *user accounts* that are linked to an *entity* . But even though this nuance would be meaningful, the fact the both terms have been used interchangeably urges caution as the reader will most probably not understand this nuance.

We recommend the usage of *identity* and the abandonment of *account* except when account is used in a fixed expression such as *Windows account* .

Related Terms

1. (link)
2. (link)
3. User Account

Quotes

> account The environment in which a user interacts with a computer system. Each account has a unique name, which the user specifies when logging in. System data associated with an account controls what resources (files, programs, networks, etc.) the user can access and in what ways (e.g. whether files that are normally writeable are read-only for particular users) and to what extent (e.g. the total size of files a user creates may be limited). Where applicable, a record can be kept of the resources used for billing purposes.

(Butterfield et al., 2016, p. 109)

((link) , p. 109)

> account authorization to use a computer or any kind of computer service, even if free of charge. An account consists of an identifying name and other records necessary to keep track of a user. Sometimes an account belongs to another computer or a computer program rather than a human being.

(Downing et al., 2009, p. 10)

((link) , p. 10)

> An entity's access to a system is encapsulated in what has become known as an account.

(Benantar, 2006, p. 3)

((link) , p. 3)

> The term user in computing has been traditionally equated with a human being. Its use conveys a unique association between a computing system and an entity that can be a human being or some programmable agent. User information is generally encapsulated in an account, sometimes referred to as a profile. A user account contains information about authentication as well as authorization credentials and may contain a set of attributes describing the user (such as a name, a serial number, an organization name, and so forth). Each user account is associated with an identifier that must be unique in the naming space of the underlying computing system.

(Benantar, 2006, p. 9)

((link) , p. 9)

Bibliography

1. (link)
2. (link)
3. (link)

See Also

false title label = "account"

Accreditation

Alternative Forms

1. Security Accreditation
2. Security Accreditation Phase

Definitions

Definition 18: Definition 1

An administrative action by which a designated authority declares that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards.

Related Terms

1. Certification

Quotes

> The Security Accreditation Phase consists of two tasks: (i) security accreditation decision; and (ii) security accreditation documentation. The purpose of this phase is to determine if the remaining known vulnerabilities in the information system (after the implementation of an agreed-upon set of security controls) pose an acceptable level of risk to agency operations, agency assets, or individuals. Upon successful completion of this phase, the information system owner will have: (i) authorization to operate the information system; (ii) an interim authorization to operate the information system under specific terms and conditions; or (iii) denial of authorization to operate the information system.(…)Completing a security accreditation ensures that an information system will be operated with appropriate management review, that there is ongoing monitoring of security controls, and that reaccreditation occurs periodically in accordance with federal or agency policy and whenever there is a significant change to the system or its operational environment.

(NIST SP 800-37, 2004, p. 2)

((link) , p. 2)

> $ accreditation(N) An administrative action by which a designated authority declares that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards. [FP102, SP37]

> (See: certification.)Tutorial: An accreditation is usually based on a technical certification of the system's security mechanisms. To accredit a system, the approving authority must determine that any residual risk is an acceptable risk. Although the terms "certification" and "accreditation" are used more in the U.S. DoD and other U.S. Government agencies than in commercial organizations, the concepts apply any place where managers are required to deal with and accept responsibility for security risks. For example, the American Bar Association is developing accreditation criteria for CAs.

(RfC 4949, 2007, p. 13)

((link) , p. 13)

Bibliography

1. (link)

See Also

label = "accreditation" false title

Access Control

Alternative Forms

AC `Acronym`

Definitions

Definition 19: Definition 1Computer Science, IAM

Restricts resource access to only authorized entities.

Related Terms

1. (link)
2. (link)
3. (link)
4. (link)
5. Control

Quotes

> Restricts resource access to only authorized entities.

(Barker, 2020, p. 6)

((link) , p. 6)

Bibliography

1. (link)

See Also

1. (link)
2. (link)
3. (link)
4. (link)

Toxic Right Rule

ARM

IAG

Identity and Access Management

Built-in

Windows Local Account

Windows NETWORK SERVICE Account

Windows HelpAssistant Account

Windows Default Local System Account

Windows DefaultAccount Account

Windows Local Administrator Account

Windows SYSTEM Account

Windows Security Identifier

Windows LOCAL SERVICE Account

Windows Default Local User Account

Windows (Non-Default) Local User Account

Privileged Identity

Core Identity

Access

Alternative Forms

1. Acc. `Abbreviation`

Definitions

Definition 20: Definition 1Noun, ability

The ability to communicate with or operate discrete functions of a system.

Definition 21: Definition 2Noun, event

The corresponding event when this ability is used.

Definition 22: Definition 3Verb

The action of using this ability.

Note

The term *access* is ambiguous as it may designate both an ability to do something or the event that results from using that ability. Speakers should pay attention to this ambiguity and assure that the context makes it clear. When the *access* ability is meant, the expression *to have access to* is less ambiguous.

Related Terms

1. (link)
2. (link)
3. (link)
4. (link)
5. Entitlement
6. (link)
7. (link)
8. (link)
9. Privilege

10. (link)
11. (link)

Quotes

> AccessTo make contact with one or more discrete functions of an online, digital service.

(NIST SP 800-63-3-R3, 2020, p. 39)

((link) , p. 39)

> $ access(I) The ability and means to communicate with or otherwise interact with a system in order to use system resources to either handle information or gain knowledge of the information the system contains.(O) "A specific type of interaction between a subject and an object that results in the flow of information from one to the other." [NCS04](C) In this Glossary, "access" is intended to cover any ability to communicate with a system, including one-way communication in either direction. In actual practice, however, entities outside a security perimeter that can receive output from the system but cannot provide input or otherwise directly interact with the system, might be treated as not having "access" and, therefore, be exempt from security policy requirements, such as the need for a security clearance.

(RfC 2828, 2000, p. 7)

((link) , p. 7)

> AccessThe ability to make use of information stored in a computer system. Used frequently as a verb, to the horror of grammarians.

(Saltzer and Schroeder, 1975)

((link))

Bibliography

1. (link)
2. (link)
3. (link)

See Also

false 50 title label = ”access”

Reference Monitor

Identity Establishment

IAM

Recertification

IMG

SoD

Definitions

Definition 23: Definition 1

An acronym of S egregation o f D uties. Cf. (link) .

Related Terms

1. (link)
2. (link)

See Also

label in (”sod” , ”segregation-of-duties”) false title

Segregation of Duties

Alternative Forms

1. SoD `Acronym`

Definitions

Definition 24: Definition 1

1 incomplete Provide definition

Related Terms

1. (link)

Quotes

2 incomplete Complete corpus research

>

(, p.)

(, p.)

Bibliography

1.

See Also

false title label in (”segregation-of-duties” , ”sod”)

Orphan Account

Alternative Forms

1. Dormant Account
2. Orphan
3. Orphaned Account
4. Uncorrelated Account

Definitions

Definition 25: Definition 1Workforce IAM

A nominative user account not linked to an active employee. Note 1 incomplete Document account removal / deactivation best practice

Definition 26: Definition 2Technical IAM

A technical account without a clearly designated account owner. Note 2 incomplete Document technical account ownership best practice

Definition 27: Definition 3IAM, Systems Requiring Declaration of User Accounts in Multiple Sub-Systems

An out of order user account because it is not declared in all the subsystems where declaration is required by the parent system. Example

In Microsoft SQL Server, users are declared in the database as *database users* and in the Microsoft SQL Server instance as *SQL logins* . A *database user* without a corresponding *SQL login* is out of order, it is an *orphaned user* . Note

Orphaned accounts constitute a security risk as they may potentially be used in unauthorized ways. In consequence the best practice consists in removing these users. See (link) .

Related Terms

1. (link)
2. Account Correlation
3. Account Owner
4. Dormant Account

5. https://open-measure.atlassian.net/wiki/spaces/DIC/pages/123830932?search_id=842b8b34-9586-4226-8b8b-f12824c7361b
6. (link)
7. Leaver Process
8. Mover Process
9. Nonperson Account
10. (link)
11. (link)
12. https://open-measure.atlassian.net/wiki/spaces/DIC/pages/67699046?search_id=d377746f-b274-4bc7-83fa-ef90d7476ae2
13. Unused Account

Quotes

> IGA concerns the capabilities in IAM market that broadly deal with end-to-end identity life-cycle management, access entitlements, workflow and policy management, role management, access certification, SOD risk analysis, reporting and access intelligence. As IGA becomes an important security risk and management discipline directly impacting the security posture of any organization, a lack of basic IGA capabilities can leave organizations exposed to risks originating from inefficient administration of identifies and access entitlements, poor role management and lack of adequate auditing and reporting. These risks range from identity thefts to unapproved and unauthorized changes, access creeps, role bloating, delays in access fulfilment, orphan roles and accounts, SOD conflicts leading to occupational and other internal frauds. Several incidents in recent past have emphasized the need to have better IGA controls for organizations of all sizes, across all industry verticals.

(Kuppinger and Hill, 2020, p. 5-6)

((link) , p. 5-6)

> Uncorrelated accountsAlso known as orphan accounts, uncorrelated accounts often occur when there's a change in an employee's status, typically when they leave the company. A good IAM system should be able to identify such accounts because they'll display an abnormal amount of inactivity. It's important to close them down because they pose a security risk. "They're ripe for attack if they're not controlled," warns Morey Haber, CTO of BeyondTrust, a maker of privileged account management and vulnerability management so-

> lutions."Many IAM programs have achieved a high level of proficiency in provisioning access to resources," adds Stealthbits' Laub. "Few, in comparison, have achieved the same level of proficiency in removing access in a complete fashion or transferring access rights when job assignments change."

(Mello, 2020)

((link))

> Correlation and Orphan AccountsAs discussed, the overall goal of an Identity Governance (IG) project is to understand and manage the relationships between people, access, and data. At the core of this goal is the logical connection between an account, token, or credential (the access) and a real human being. The ongoing process of connecting people to accounts and access is called correlation and is shown in Figure 7-1. In the ideal world, every account matches up perfectly with a human (identity), and you have 100% correlation (for the record, that's something we never see out of the gate). Account access that does not correlate back to a known user is often referred to as an orphan account. Orphan accounts can be a significant security weakness. Post-breach forensic analysis shows that the adversary creates and uses new accounts throughout the cyber killing chain. It is therefore essential for ongoing governance and security to instrument, and, if at all possible, to automate, the detection and rapid resolution of orphan accounts.The presence of system, functional, privileged, and application accounts poses a significant challenge to this process. The accounts and privileges used for system-to-system access and the administration of the IT infrastructure are rarely if ever directly correlatable to a known user without a dedicated process. In large ecosystems, there can be hundreds and potentially thousands of accounts that will not correlate without a deliberate and specific process of managed correlation. An enterprise-grade IG solution will provide core product capabilities to help either manually or automatically resolve these issues. Manual correlation using graphical "searching and connecting" will greatly help the admin establish and maintain links between known owners and orphan accounts. Automated matching algorithms can also help suggest relationships and potential connections. This automated discovery technology can also provide important insights around the integration with Privileged Account Management (PAM) solutions. Finding privilege and directing the PAM solution to take control of the account can be a significant win. Chapter 13 provides more details on the best practices around the integration between PAM and IG solutions.

(Haber and Rolls, 2020, p. 58-59)

((link) , p. 58-59)

> IGA(…) • Identification of dormant/orphan accounts

(Diodati and Ruddy, 2017, p. 17-18)

((link) , p. 17-18)

> Lack of Business AlignmentThis is commonly understood as a problem, but difficult to address. Most presentations that Gartner reviewed ignore the business impact beyond generally tying it to FUD. Those that do address it make poor connections between security problems and business impact, such as orphan accounts that negatively affect profitability. This leads to a lack of credibility and defensibility, and erodes board support, perpetuating the notion that this is not the board's issue (see "Five Tips for Security and Risk Leaders When Communicating With Business Stakeholders").

(Proctor et al., 2017, p. 7)

((link) , p. 7)

> Another significant security concern is identity life cycle and de-provisioning. When people leave the organization, who removes their accounts and permissions on cloud services? This removal can be a considerable identity management challenge, and is a major business driver for enterprises deploying identity and access management capabilities. In the absence of automation, the enterprise will have to rely on manual procedures. With manual procedures, periodic audits should be performed to clean up orphan accounts and excessive permissions.

(Donaldson et al., 2015, p. 115)

((link) , p. 115)

> The business can also provide input on whether all accounts reviews are properly assigned. This is particularly important when managing orphan and nonperson accounts that require an owner for designation prior to review. An orphan account is an account belonging to a user who has since left the organization.To help support the cleanup of orphan accounts, coordination and support are typically leveraged from a combination of system teams, application teams, and business owners to identify and properly associate the correct individuals to maintain accountability for the account.

(Gazos and Osmanoglu, 2013, 454-455)

((link) , 454-455)

> 6.6 Configuration vulnerabilities (Category VCF)(…)Indicators associated with events belonging to this category measure the frequency of occurrence of these vulnerabilities, highlighting deviations in the application of the standard security policy by network or system administrators or shortcomings of these standard configurations. For that purpose, 9 special kinds of configuration vulnerabilities have been selected (representing 5 different families):(…) • Family VCF_UAC (Access rights not compliant with the security policy, access rights on logs in servers which are sensitive and/or subject to regulations not compliant with the security policy, generic and shared administrator accounts that are unnecessary or accounts that are necessary but without patronage accounts without owners – dormant or orphan accounts – that have not been erased, accounts inactive for at least 2 months that have not been disabled)

(ETSI GS ISI 002, 2013 ,p. 32-33)

((link) ,p. 32-33)

> Assess Identity RisksOrganizations that are able to identify and assess identity related risks are said to be in a better position to protect their intellectual property (IP). User access to applications should have a clear process for granting access with emphasis on associated business risks. . Some of the risks arising from orphan accounts, shared accounts, test accounts and accounts of temporary workers are often not handled effectively. One of the options to handle risk is to first assign scores to the risks associated with each of the applications and their entitlements. Once the risk scoring is in place, collecting this data and combining it with the identity data will help in identification of high risk profiles. Additionally, effective Joiner-Mover-Leaver (JML) processes and monitoring of policy violations across applications help in reducing risks and maintaining control.By utilizing the identity intelligence gathered as part of the IAG program, threats from insiders can be addressed by initiating proactive measures. For example, if an employee with high risk value is expected to be terminated from service, then steps can be taken to curtail his access before his actual termination date.

(Hurakadli and Sridhar, 2012, p. 5)

((link) , p. 5)

> A database user for which the corresponding SQL Server login is undefined or is incorrectly defined on a server instance cannot log in to the instance. Such a user is said to be an orphaned user of the database on that server instance.

> A database user can become orphaned if the corresponding SQL Server login is dropped. Also, a database user can become orphaned after a database is restored or attached to a different instance of SQL Server. Orphaning can happen if the database user is mapped to a SID that is not present in the new server instance.

(Microsoft, 2010)

((link))

Bibliography

1. (link)
2. (link)
3. (link)
4. (link)
5. (link)
6. (link)
7. (link)
8. (link)
9. (link)
10. (link)

See Also

false title label in (”orphan” , ”orphan-account” , ”orphaned-account” , ”uncorrelated-account”)

Orphan Product

Alternative Forms

1. Orphan

Definitions

Definition 28: Definition 1IT Service Management

A IT product that is no longer supported or whose editor or manufacturer ceased to exist.

Related Terms

1. (link)
2. Product

Quotes

> orphan(…)2. a computer product that is no longer supported by its manufacturer, or whose manufacturer is out of business. For example, the Amiga is now an orphan computer.

(Downing et al., 2009, p. 345)

((link) , p. 345)

Bibliography

1. (link)

See Also

label = ”orphan-product” false title

Orphan File

Alternative Forms

1. Orphan

Definitions

Definition 29: Definition 1Computer Science

A file whose owner has been deleted.

Related Terms

1. File
2. (link)

Quotes

> Once you have removed a user, you may want to verify that the user's old UID no longer owns files on the system. To find the paths of orphaned files, you can use the find command with the -nouser argument. Because find has a way of "escaping" onto network servers if you're not careful, it's usually best to check filesystems individually with -xdev:$ sudo find filesystem -xdev -nouser

(Nemeth et al., 2011, p. 198)

((link) , p. 198)

Bibliography

1. (link)

See Also

label = "orphan-file" false title

Orphan Process

Alternative Forms

1. Orphan

Definitions

Definition 30: Definition 1Computer Science, Linux

In Linux, a process whose parent is dead. An orphan process is automatically made a child of init.

Related Terms

1. Linux
2. (link)
3. Process
4. UNIX

Quotes

> Before a process can be allowed to disappear completely, the kernel requires thatits death be acknowledged by the process's parent, which the parent does with acall to wait. The parent receives a copy of the child's exit code (or an indication ofwhy the child was killed if the child did not exit voluntarily) and can also obtain asummary of the child's use of resources if it wishes.This scheme works fine if parents outlive their children and are conscientiousabout calling wait so that dead processes can be disposed of. If the parent diesfirst, however, the kernel recognizes that no wait will be forthcoming and adjustsths the process to make the orphan a child of init. init politely accepts these orphanedprocesses and performs the wait needed to get rid of them when they die.

(Nemeth et al., 2011, p. 124)

((link) , p. 124)

Bibliography

1. (link)

See Also

label = ”orphan-process” false title

Orphan System

Alternative Forms

1. Orphan

Definitions

Definition 31: Definition 1IT Service Management

An IT system without a system owner.

Notes

Because nobody is responsible for an *orphan system* , the satisfaction of system requirements is no longer assured. This represent an operational risk, including a security risk.

Related Terms

1. (link)
2. https://open-measure.atlassian.net/wiki/spaces/DIC/pages/1004961963?search_id=ae11927e-ff6c-45df-af8d-26c57376ff39

Quotes

> It is the responsibility of the information security manager to ensure that, in the assignment process, there are no “orphan” systems or systems without policy-compliance owners.

(ISACA, 2012, p. 175)

((link) , p. 175)

Bibliography

1. (link)

See Also

false title label = ”orphan-system”

Orphan Routes / APIs

Alternative Forms

1. Orphan

Definitions

Definition 32: Definition 1Computer Science

Deprecated or abandoned parts of an application. Orphan Routes / APIs constitute a typical security blind spot.

Related Terms

1. File
2. (link)

Quotes

> Orphan routes and APIs representing security blind spots. “Dead code”, also known as orphan routes/APIs are deprecated or abandoned parts of (web) applications with zero business purpose or value, in other words: “blind spots”. Thus, the increase in usage of APIs and the business interconnectivity concepts affects the attack surface (cause by blind spots) to rise exponentially147.

(ENISA, 2019 , p. 37)

((link) , p. 37)

Bibliography

1. (link)

See Also

false title label = ”orphan-file”

Orphan Object

Alternative Forms

1. Orphan

Definitions

Definition 33: Definition 1Computer Science, Memory Management

An object instance that is no longer referenced.

Related Terms

1. Object
2. (link)

Quotes

> Orphaned objects. The ability to assign different objects to a reference variable creates the possibility that a program may have created an object that it can no longer reference. For example, consider the three assignment statements in the figure at right. After the third assignment statement, not only do a and b refer to the same Color object (the one whose RGB values are 160, 82, and 45), but also there is no longer a reference to the Color object that was created and used to initialize b. The only reference to that object was in the variable b, and this reference was overwritten by the assignment, so there is no way to refer to the object again. Such an object is said to be orphaned. Objects are also orphaned when they go out of scope. Java programmers pay little attention to orphaned objects because the system automatically reuses the memory that they occupy, as we discuss next.

(Sedgewick and Wayne, 2017, p. 366)

((link) , p. 366)

Bibliography

1. (link)

See Also

label = ”orphan-object” false title

Orphan

Definitions

Definition 34: Definition 1Compute Science

In Computer Science, the term *orphan* may refer to the abbreviated form of multiple distinct concepts:

1. Orphan Account `Computer Science, Cybersecurity, IAM`
2. Orphan File `Computer Science, Operating System`
3. Orphan Object `Computer Science, Memory Management`
4. Orphan Process `Computer Science, Operating System`
5. Orphan Product `IT Service Management`
6. Orphan Role `Computer Science, Cybersecurity, IAM`
7. Orphan Routes / APIs `Computer Science, Cybersecurity, Application Management`
8. Orphan System `IT Service Management`

Definition 35: Definition 2Computer Science

A process or computation without recipient.

Definition 36: Definition 3Digital Forensics

A data fragment that is no longer linked to its normal structure, such as a deleted file.

Related Terms

1. (link)
2. (link)
3. (link)
4. (link)
5. (link)
6. (link)
7. (link)
8. (link)

Quotes

> As an example, Forensic Toolkit (FTK) recovers deleted files and folders from ext2 file systems into an area called “[orphan],” organizing and displaying the recovered data in a way that facilitates examination.

(Casey, 2011, p. 569)

((link) , p. 569)

> orphan a process or computation for which no recipients exist.

(Laplante, 2001, p. 351)

((link) , p. 351)

Bibliography

1. (link)

See Also

false title label = ”orphan”

IAM ARN

Definitions

Definition 37: Definition 1AWS

The ARN of an AWS IAM object, in the form: `arn:partition:service:region:account:resource` .

Related Terms

1. ARN
2. AWS
3. URN

Quotes

> IAM ARNsMost resources have a friendly name (for example, a user named Bob or a group named Developers). However, the permissions policy language requires you to specify the resource or resources using the following Amazon Resource Name (ARN) format.arn:partition:service:region:account:resource

(AWS, 11/2020, p. 597)
(Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_identifiers.html#identifiers-arns)

((link) , p. 597) (Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_identifiers.html#arns)

Bibliography

1. (link)

See Also

false title label = ”iam-arn”

Access Continuum

Definitions

Definition 38: Definition 1

Entities have varying levels of access to organizations' resources. The binary classification *insider* versus *outsider* is a highly simplified model. In contrast, considering access levels as a continuum allows for a more sophisticated model and may help focus on the most critical aspect: access, rather than statute.

Illustration

Related Terms

1. (link)
2. Continuum
3. Insider
4. Insider Threat
5. Level of Access
6. Outsider
7. Outsider Threat

Quotes

> Our theme is that the distinction between "insider" and "outsider" is not binary; rather, there are "attackers" with varying degrees and types of access. One can call some set of these attackers "insiders," with the complement being the "outsiders," but countermeasures should focus on the access and not on whether the attackers are insiders. Thus, we see attacks as spanning a continuum of levels and types of access, and use that as the basis of our discussion. We emphasize that people comfortable thinking in terms of "insiders" and "outsiders" can superimpose that partition on our notion of "attackers with varying levels of access." That partition, however, will vary based on circumstances and environment.

(Bishop et al., 2010, p. 117)

((link) , p. 117)

Bibliography

1. (link)

See Also

false title label = ”access-continuum”

Unanticipated User

Definitions

Definition 39: 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

1. ABAC
2. (link)
3. Identity Federation
4. Onboarding Process
5. PBAC
6. Unanticipated Entity `Generic Form`
7. (link)

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)

((link) , p. 3)

Bibliography

1. (link)

See Also

false title label = ”unanticipated-user”

Access Granularity

Definitions

Definition 40: Definition 1

Access granularity designates the scale or precision level(s) at which access control is supported by a system.

A system that supports finer grained access controls may provide more configurational flexibility but may require higher maintenance costs, unless it provides efficient mechanisms to simplify and automate access management. Conversely, a system that supports coarser grained access controls may provide less configurational flexibility but may require lower maintenance costs.

A system may simultaneously support multiple access granularity levels. When loosely speaking about the granularity of a system, the intention is often to get a sense of the flexibility provided by a system and thus the smallest level is generally implied. Examples

1. a file server may support file-level ACLs as its smallest access granularity.
2. a relational database management system may support database-level, table-level, row-level and field-level access granularities.
3. a business application may implement complex policy-based access control mechanisms that resolve in a matrix of record and operation access granularity levels where both record and operation accesses are required to gain access.

Related Terms

1. Access
2. Authorization
3. Coarse-Grained Access Controls
4. Fine-grained Access Controls
5. Information Asset
6. Information Asset Granularity

Quotes

> Degree of Granularity – Typically, more simplistic structures such as ACLs or IBAC may be adequate when coarse access decisions are needed, such as the ability to gain access to an enterprise based on membership in an organization. On the other hand, implementing fine-grained controls may be more suitable for granting access to information, where many factors may have to be considered to implement formal release policies established for each information object requested. Here an ABAC or PBAC structure may be more suitable.

(Farroha and Farroha, 2012, p. 3)

((link) , p. 3)

> Access granularity defines the storage unit to control data access – e.g., at the tuple, tables or databases levels.

(Sasaoka and Medeiros, 2006, p. 111)

((link) , p. 111)

> 6.1.3 The degree to which an access control system supports the concept of least privilegeIn addition to an access control mechanism's reference mediation function, there are two other basic functions: a function to create subjects and associate these subjects with their users, and a function to associate a subject with a subset of attributes that are assigned to its user. Regardless of its implementation and the type of attributes that are deployed, reference mediation of an access control system constrains the subject and user's requests to the capabilities that are associated with a subject's attributes. Although a number of access control mechanisms associate a subject with each and every user attribute, in order for an access control mechanism to support the principle of least privilege, constraints must be placed on the attributes that are associated with a subject to further reduce the permissible capabilities. The organization specific least- privilege policy is described by specifying the rules composed by the basic access control elements: subjects, operations, and objects. The access control systems provide various specifying methods, which achieve different degrees of granularity, flexibility, and scope, and different groupings of the controlled resources for the least-privilege policies.

(NIST IR 7316, 2006, p. 37)

((link) , p. 37)

> 4.2.7 GranularityA practical problem with all current flavors of access control system is granularity. As the operating system works with files, this will usually be the smallest object with which its access control mechanisms can deal. So it will be application-level mechanisms that, for example, ensure that a bank customer at a cash machine can see his or her own balance but not anybody else's.But it goes deeper than that. Many applications are built using database tools that give rise to some problems that are much the same whether running DB2 on MVS or Oracle on Unix. All the application data is bundled together in one file, and the operating system must either grant or deny a user access to the lot. So, if you developed your branch accounting system under a database product, then you'll probably have to manage one access mechanism at the operating system level and another at the database or application level. Many real problems result. For example, the administration of the operating system and the database system may be performed by different departments, which do not talk to each other; and often user pressure drives IT departments to put in crude hacks that make the various access control systems seem to work as one, but that open up serious holes. Another granularity problem is single sign-on. Despite the best efforts of computer managers, most large companies accumulate systems of many different architectures, so users get more and more logons to different systems; consequently, the cost of administering them escalates. Many organizations want to give each employee a single logon to all the machines on the network. A crude solution is to endow their PCs with a menu of hosts to which a logon is allowed, and hide the necessary userids and passwords in scripts. More sophisticated solutions may involve a single security server through which all logons must pass, or a smartcard to do multiple authentication protocols for different systems. Such solutions are hard to engineer properly. Whichever route one takes, the security of the best system can easily be reduced to that of the worst.

(Anderson, 2001,p. 60-61)

((link) ,p. 60-61)

> An operation represents a unit of control that can be referenced by an individual role that is subject to regulatory constraints within the RBAC framework. It is important to note the difference between a simple mode of access and an operation. An operation can be used to capture security-relevant details or constraints that cannot be determined by a simple mode of access[2]. These details can be in terms of both method and granularity of access.

(Ferraiolo, 1995, p. 3)

((link) , p. 3)

Bibliography

1. (link)
2. (link)
3. (link)
4. (link)
5. (link)

See Also

false 50 title label = ”access-granularity”
Book end