Autorización

La autorización o **autorización** (ver diferencias ortográficas) es la función de especificar derechos/privilegios para acceder a recursos, que está relacionada con la seguridad general de la información y la seguridad informática , y con IAM (Gestión de identidad y acceso) en particular. [1] De manera más formal, "autorizar" es definir una política de acceso durante la configuración de sistemas y cuentas de usuario. Por ejemplo, las cuentas de usuario para el personal de recursos humanos suelen configurarse con autorización para acceder a los registros de los empleados, y esta política se formaliza como reglas de control de acceso en un sistema informático. La autorización no debe confundirse con el control de acceso. Durante el uso, el control de acceso hace cumplir la política de autorización al decidir si las solicitudes de acceso a los recursos de los consumidores (autenticados) se aprobarán (concederán) o rechazarán (rechazarán). [2] Los recursos incluyen archivos individuales o datos de un elemento , programas informáticos , dispositivos informáticos y funcionalidad proporcionada por aplicaciones informáticas . Ejemplos de consumidores son los usuarios de computadoras, el software de computadoras y otro hardware en la computadora.

Descripción general

IAM consists the following two phases: the configuration phase where a user account is created and its corresponding access authorization policy is defined, and the usage phase where user authentication takes place followed by access control to ensure that the user/consumer only gets access to resources for which they are authorized. Hence, access control in computer systems and networks relies on access authorization specified during configuration.

Most modern, multi-user operating systems include role-based access control (RBAC) where authorization is implicitly defined by the roles. User authentication is the process of verifying the identity of consumers. When an authenticated consumer tries to access a resource, the access control process checks that the consumer has been authorized to use that resource. Authorization is the responsibility of an authority, such as a department manager, within the application domain, but is often delegated to a custodian such as a system administrator. Authorizations are expressed as access policies in some types of "policy definition application", e.g. in the form of an access control list or a capability, or a policy administration point e.g. XACML. On the basis of the "principle of least privilege": consumers should only be authorized to access whatever they need to do their jobs. Older and single user operating systems often had weak or non-existent authentication and access control systems.

"Anonymous consumers" or "guests", are consumers that have not been required to authenticate. They often have limited authorization. On a distributed system, it is often desirable to grant access without requiring a unique identity. Familiar examples of access tokens include keys, certificates and tickets: they grant access without proving identity.

Trusted consumers are often authorized for unrestricted access to resources on a system, but must be verified so that the access control system can make the access approval decision. "Partially trusted" and guests will often have restricted authorization in order to protect resources against improper access and usage. The access policy in some operating systems, by default, grant all consumers full access to all resources. Others do the opposite, insisting that the administrator explicitly authorizes a consumer to use each resource.

Even when access is controlled through a combination of authentication and access control lists, the problems of maintaining the authorization data is not trivial, and often represents as much administrative burden as managing authentication credentials. It is often necessary to change or remove a user's authorization: this is done by changing or deleting the corresponding access rules on the system. Using atomic authorization is an alternative to per-system authorization management, where a trusted third party securely distributes authorization information.

Interpretaciones relacionadas

Public policy

In public policy, authorization is a feature of trusted systems used for security or social control.

Banking

In banking, an authorization is a hold placed on a customer's account when a purchase is made using a debit card or credit card.

Publishing

In publishing, sometimes public lectures and other freely available texts are published without the approval of the author. These are called unauthorized texts. An example is the 2002 *'The Theory of Everything: The Origin and Fate of the Universe'*, which was collected from Stephen Hawking's lectures and published without his permission as per copyright law.

Véase también

- Access control
- Authorization hold
- Authorization OSID
- Kerberos (protocol)
- Multi-party authorization
- OAuth
- OpenID Connect
- OpenID
- Usability of web authentication systems
- WebFinger
- WebID
- XACML

Referencias

1. Fraser, B. (1997), *RFC 2196 – Site Security Handbook*, IETF
2. Jøsang, Audun (2017), *A Consistent Definition of Authorization*, Proceedings of the 13th International Workshop on Security and Trust Management (STM 2017)