**Access control principals**

**Identification:**For access control to be effective, it must provide some way to identify an individual. The weakest identification capabilities will simply identify someone as part of a vague, poorly defined group of users who should have access to the system. Your TechRepublic username, a PGP e-mail signature, or even the key to the server closet provides some form of identification.

**Authentication:** Identification requires authentication. This is the process of ensuring that the identity in use is authentic -- that it's being used by the right person. In its most common form in IT security, authentication involves validating a password linked to a username. Other forms of authentication also exist, such as fingerprints, smartcards, and encryption keys.

**Authorization:** The set of actions allowed to a particular identity makes up the meat of authorization. On a computer, authorization typically takes the form of read, write, and execution permissions tied to a username.

**Access control model**

**Access control models** have four flavors: Mandatory **Access Control** (MAC), Role Based **Access Control** (RBAC), Discretionary **Access Control** (DAC), and Rule Based **Access Control** (RBAC or RB-RBAC)

**ACL**

An access control list (ACL) contains rules that grant or deny access to certain digital environments. There are two types of ACLs:

**Filesystem ACLs :** filter access to files and/or directories. Filesystem ACLs tell operating systems which users can access the system, and what privileges the users are allowed.

**Networking ACLs :** filter access to the network. Networking ACLs tell routers and switches which type of traffic can access the network, and which activity is allowed.

Reasons to use an ACL:

* Traffic flow control
* Restricted network traffic for better network performance
* A level of security for network access specifying which areas of the server/network/service can be accessed by a user and which cannot
* Granular monitoring of the traffic exiting and entering the system

**DAC**

Discretionary access control (DAC) is a type of security access control that grants or restricts object access via an access policy determined by an object's owner group and/or subjects. DAC mechanism controls are defined by user identification with supplied credentials during authentication, such as username and password. DACs are discretionary because the subject (owner) can transfer authenticated objects or information access to other users. In other words, the owner determines object access privileges.

**DAC attributes include:**

* User may transfer object ownership to another user(s).
* User may determine the access type of other users.
* After several attempts, authorization failures restrict user access.
* Unauthorized users are blind to object characteristics, such as file size, file name and directory path.
* Object access is determined during access control list (ACL) authorization and based on user identification and/or group membership.

**DAC is easy to implement and intuitive but has certain disadvantages, including:**

* Inherent vulnerabilities (Trojan horse)
* ACL maintenance or capability
* Grant and revoke permissions maintenance
* Limited negative authorization power

**MAC**

A message authentication code system consists of three algorithms:

* A key generation algorithm selects a key from the key space uniformly at random.
* A signing algorithm efficiently returns a tag given the key and the message.
* A verifying algorithm efficiently verifies the authenticity of the message given the key and the tag. That is, return accepted when the message and tag are not tampered with or forged, and otherwise return rejected.

**Implementation :**

MAC algorithms can be constructed from other cryptographic primitives, like cryptographic hash functions (as in the case of HMAC) or from block cipher algorithms (OMAC, CCM, GCM, and PMAC). However many of the fastest MAC algorithms like UMAC-VMAC and Poly1305-AES are constructed based on universal hashing.[7]

Intrinsically keyed hash algorithms such as SipHash are also by definition MACs; they can be even faster than universal-hashing based MACs.

Additionally, the MAC algorithm can deliberately combine two or more cryptographic primitives, so as to maintain protection even if one of them is later found to be vulnerable. For instance, in Transport Layer Security (TLS), the input data is split in halves that are each processed with a different hashing primitive (SHA-1 and SHA-2) then XORed together to output the MAC.

**Role based Access control**

Role-based access control (RBAC) restricts network access based on a person's role within an organization and has become one of the main methods for advanced access control. The roles in RBAC refer to the levels of access that employees have to the network.

Through RBAC, you can control what end-users can do at both broad and granular levels. You can designate whether the user is an administrator, a specialist user, or an end-user, and align roles and access permissions with your employees’ positions in the organization. Permissions are allocated only with enough access as needed for employees to do their jobs.

**Advantages :**

* Reducing administrative work and IT support
* Maximizing operational efficiency
* Improving compliance

**Kerberos**

Kerberos is a computer network security protocol that authenticates service requests between two or more trusted hosts across an untrusted network, like the internet. It uses secret-key cryptography and a trusted third party for authenticating client-server applications and verifying users’ identities.

What is the main feature of Kerberos?

The Kerberos protocol uses a unique ticketing system that provides faster authentication: Every authenticated domain entity can request tickets from its local Kerberos KDC to access other domain resources. The tickets are considered as access permits by the resource servers.

What are the 3 main parts of Kerberos?

Kerberos has three parts: a client, server, and trusted third party (KDC) to mediate between them. Clients obtain tickets from the Kerberos Key Distribution Center (KDC), and they present these tickets to servers when connections are established.