MS Windows 10 Access Control

Name : Anwor Bashir Rajab Diab

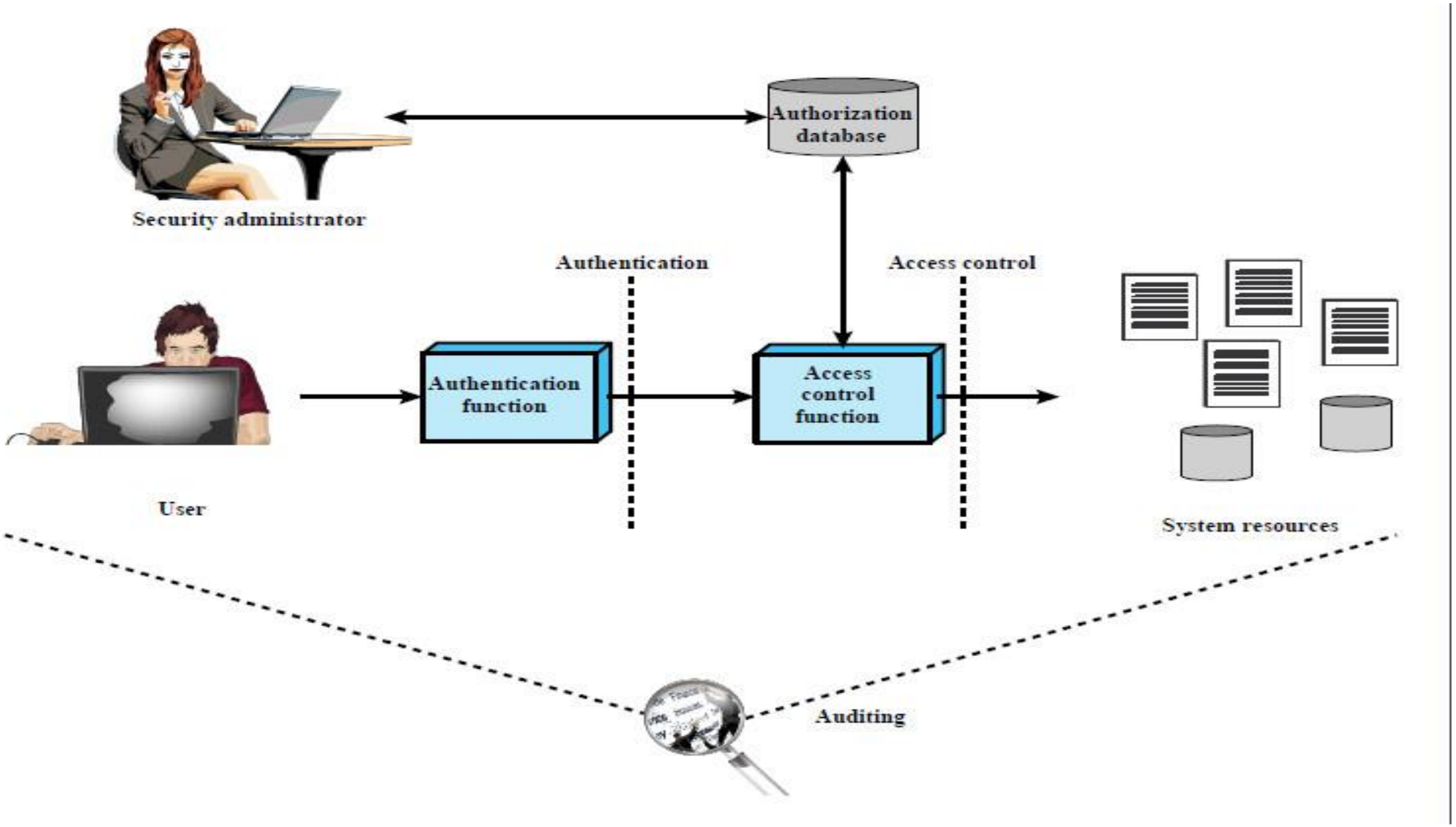
ID : 163104008

Supervisor : Prof. Dr. Hasan Huseyin Balik

Outline :

- **What is Access Control .**
- **Windows System Accounts .**
- **Windows User Accounts .**
- **What are security identifiers .**
- **How security identifiers work .**
- **Security identifier architecture .**
- **Access Control Methods .**
- **How security principals work .**
- **Authorization and access control components .**
- **Accounts and security groups .**
- **User accounts and Security groups .**
- **Conclusion .**

What is Access Control ?



After a user is authenticated, the Windows operating system uses the authorization to

Determining if an authenticated user has the correct permissions to access a resource .

Windows System Accounts :

The user mode components of the kernel of the Windows operating system (e.g., *csrss.exe* and *lsass.exe*) run under the *Local System* account.

This account has complete access to all the resources of the machine and most of the daemon programs run under this account.

a global hierarchical database to store data from all programs . over the network.

The operating system service responsible for responding to remote registry requests runs as *Local Service*. (Even though *Local Service* does not have complete access to the registry, it can use Windows's delegation facility to access the registry on behalf of the client.)

One cannot login into the accounts *Local System*, *Local Service* and *Network Service*, but can control these accounts from any account in the *Administrators* group.

Windows User Accounts :

The *Administrator* account is the account one uses upon first setting up, before creating any other account .

It is a member of the *Administrators* group. Any member of the *Administrators* group has complete control of the machine.

Windows has various other groups, such as *Authenticated Users*, *Everyone*, *Server Operators*, *Power Users* , *Network Conjuration Operators*.

Members of the *Power Users* group can create user accounts, can modify and delete accounts they create, stop and start system services which are not started by default .

What are security identifiers ?

A security identifier (SID) is used to uniquely identify a security principal or security group. Security principals can represent any entity that can be authenticated by the operating system, such as a user account, a computer account, or a thread or process that runs in the security context of a user or computer account.

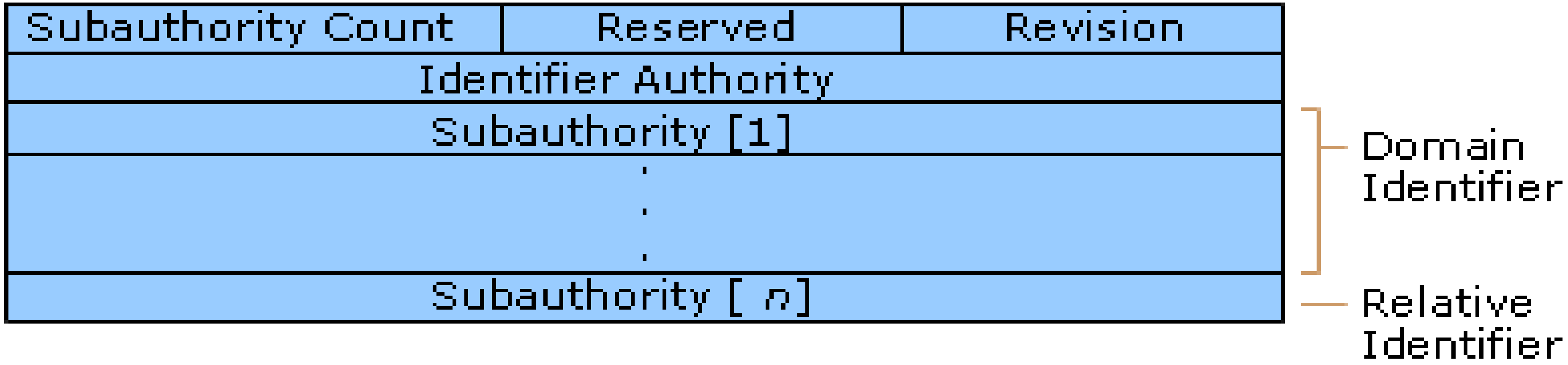
How security identifiers work ?

Users refer to accounts by using the account name, but the operating system internally refers to accounts and processes that run in the security context of the account by using their security identifiers (SIDs). For domain accounts, the SID of a security principal is created by concatenating the SID of the domain with a relative identifier (RID) for the account.

Security identifier architecture .

A security identifier is a data structure in binary format that contains a variable number of values. The first values in the structure contain information about the SID structure. The remaining values are arranged in a hierarchy (similar to a telephone number), and they identify the SID-issuing authority.

The following image illustrates the structure of a SID.



The components of a SID are easier to visualize when SIDs are converted from a binary to a string format by using standard notation :

S-R-X-Y1-Y2-Yn-1-Yn

In this notation, the components of a SID are represented as shown in the following table .

Comment	Description
S	Indicates that the string is a SID
R	Indicates the revision level
X	Indicates the identifier authority value
Y	Represents a series of subauthority values, where n is the number of values

For example, the SID for the built-in Administrators group is represented in standardized SID notation as the following string :

S-1-5-32-544

This SID has four components :

- A revision level (1)
- An identifier authority value (5, NT Authority)
- A domain identifier (32, Builtin)
- A relative identifier (544, Administrators)

Access Control Methods :

- **Access Control Matrices .**

– Disadvantage: In a large system, the matrix will be enormous in size and mostly sparse .

- **Access Control List .**

– The column of access control matrix.

  – Advantage :

    * Easy to determine who can access a given object.

    * Easy to revoke all access to an object

  – Disadvantage :

    * Difficult to know the access right of a given subject.

    * Difficult to revoke a user’s right on all objects.

– Used by most mainstream operating systems.

How security principals work .

Security principals that are created in an Active Directory domain are Active Directory objects, which can be used to manage access to domain resources. Each security principal is assigned a unique identifier, which it retains for its entire lifetime.

Local user accounts and security groups are created on a local computer, and they can be used to manage access to resources on that computer.

Local user accounts and security groups are managed by the Security Accounts Manager (SAM) on the local computer .

Accounts and security groups .

Accounts and security groups that are created in an Active Directory domain are stored in the Active Directory database and managed by using Active Directory tools .These security principals are directory objects, and they can be used to manage access to domain resources .

Local user accounts and security groups are created on a local computer, and they can be used to manage access to resources on that computer .

Local user accounts and security groups are stored in and managed by the Security Accounts Manager (SAM) on the local computer .

User accounts .

A user account uniquely identifies a person who is using a computer system. The account signals the system to enforce the appropriate authorization to allow or deny that user access to resources. User accounts can be created in Active Directory and on local computers, and administrators use them to:

- Represent, identify, and authenticate the identity of a user. A user account enables a user to sign in to computers, networks, and domains with a unique identifier that can be authenticated by the computer, network, or domain.
- Authorize (grant or deny) access to resources. After a user has been authenticated, the user is authorized access to resources based on the permissions that are assigned to that user for the resource.
- Audit the actions that are carried out on a user account.

Security groups .

A security group is a collection of user accounts, computer accounts, and other groups of accounts that can be managed as a single unit from a security perspective .

In Windows operating systems, there are several built-in security groups that are preconfigured with the appropriate rights and permissions for performing specific tasks .

Additionally, you can (and, typically, will) create a security group for each unique combination of security requirements that applies to multiple users in your organization .

Conclusion :

Access Control in Windows is designed as a Discretionary Access Control model that is fitted to act as a Role-Based Access Control model due to its groups and administrative privileges’ capabilities. Groups can be regarded as roles, permissions and privileges can be assigned to these groups/roles, and finally users can be joined to the said groups/roles.

. Thank you .