Authentication and authorization are two vital information security processes that administrators use to protect systems and information. Authentication verifies the identity of a user or service, and authorization determines their access rights. Although the two terms sound alike, they play separate but equally essential roles in securing applications and data. Understanding the difference is crucial. Combined, they determine the security of a system. You cannot have a secure solution unless you have configured both authentication and authorization correctly.

What is Authentication (AuthN)?

Authentication (AuthN) is a process that verifies that someone or something is who they say they are. Technology systems typically use some form of authentication to secure access to an application or its data.

For example, when you need to access an online site or service, you usually have to enter your username and password. Then, behind the scenes, it compares the username and password you entered with a record it has on its database. If the information you submitted matches, the system assumes you are a valid user and grants you access. System authentication in this example presumes that only you would know the correct username and password. It, therefore, authenticates you by using the principle of something only you would know.

What is the Purpose of Authentication?

The purpose of authentication is to verify that someone or something is who or what they claim to be. There are many forms of authentication. For example, the art world has processes and institutions that confirm a painting or sculpture is the work of a particular artist. Likewise, governments use different authentication techniques to protect their currency from counterfeiting. Typically, authentication protects items of value, and in the information age, it protects systems and data.

What is Identity Authentication?

Identity authentication is the process of verifying the identity of a user or service. Based on this information, a system then provides the user with the appropriate access. For example, let's say we have two people working in a coffee shop, Lucia and Rahul. Lucia is the coffee shop manager while Rahul is the barista. The coffee shop uses a Point of Sale (POS) system where waiters and baristas can place orders for preparation. In this example, the POS would use some process to verify Lucia or Rahul's identity before allowing them access to the system. For instance, it may ask them for a username and password, or they may need to scan their thumb on a fingerprint reader. As the coffee shop needs to secure access to its POS, employees using the system need to verify their identity via an authentication process.

Common Types of Authentication

Systems can use several mechanisms to authenticate a user. Typically, to verify your identity, authentication processes use: - something you know - something you have - or something you are

Passwords and security questions are two authentication factors that fall under the something-you-know category. As only you would know your password or the answer to a particular set of security questions, systems use this assumption to grant you access.

Another common type of authentication factor uses something you have. Physical devices such as USB security tokens and mobile phones fall under this category.

For example, when you access a system, and it sends you a One Time Pin (OTP) via SMS or an app, it can verify your identity because it is your device.

The last type of authentication factor uses something you are. Biometric authentication mechanisms fall under this category. Since individual physical characteristics such as fingerprints are unique, verifying individuals by using these factors is a secure authentication mechanism.

What is Authorization (AuthZ)?

Authorization is the security process that determines a user or service's level of access. In technology, we use authorization to give users or services permission to access some data or perform a particular action.

If we revisit our coffee shop example, Rahul and Lucia have different roles in the coffee shop. As Rahul is a barista, he may only place and view orders. Lucia, on the other hand, in her role as manager, may also have access to the daily sales totals. Since Rahul and Lucia have different jobs in the coffee shop, the system would use their verified identity to provide each user with individual permissions.

It is vital to note the difference here between authentication and authorization. Authentication verifies the user (Lucia) before allowing them access, and authorization determines what they can do once the system has granted them access (view sales information).

Common Types of Authorization

Authorization systems exist in many forms in a typical technology environment. For example, Access Control Lists (ACLs) determine which users or services can access a particular digital environment.

They accomplish this access control by enforcing allow or deny rules based on the user's authorization level. For instance, on any system, there are usually general users and super users or administrators.

If a standard user wants to make changes that affect its security, an ACL may deny access.

On the other hand, administrators have the authorization to make security changes, so the ACL will allow them to do so.

Another common type of authorization is access to data. In any enterprise environment, you typically have data with different levels of sensitivity. For example, you may have public data that you find on the company's website, internal data that is only accessible to employees, and confidential data that only a handful of individuals can access. In this example, authorization determines which users can access the various information types.