Lesson 4: Types of Authentication and Access Control

by Justin David Pineda

Authentication

Authentication is defined as proving who you are claiming to be. By default, we have 3 types of authentication:

1. Something that you know – A form of authentication coming from what you know (residing in the mind)
   Ex. Password, pin
2. Something that you have – A form of authentication that is tangible.
   Ex. Token, cellphone, ID
3. Something that you are – A form of authentication where the uniqueness of the part of your body is used.
   Ex. Fingerprint, voice recognition, iris scan

Not one of the authentication types can be considered the strongest. *Something that you know* authentication such as password can be cracked using brute force or social engineering. *Something that you have authentication* such as ID's can be stolen or reproduced. *Something that you are* authentication such fingerprint is prone to false positives (you have sweaty hands etc.)

To make your authentication stronger, it is advised that you use 2 or more types of authentication to provide a layer of security. This is what we call 2-factor or multi-factor authentication. Examples include:

1. ATM + Pin (something that you have and you know)
2. Credit card + signature (something that you have and you know)
3. Cellphone for One-Time Password (OTP) + password (something that you have and you know)
4. Badge + biometric (something that you have and you are)

Note: Usernames and passwords are not considered multi-factor because both are something that you know type of authentication.

Questions to search on:

1. What is the fourth type (or other types) of authentication?
2. What is the most accurate biometric? Why?

Types of Access Control

Access Control or Authorization determines the type of privilege a user has after being authenticated. If you enter the school, an authentication mechanism could be your school ID. Access Control determines which rooms in the school you can access. If you're a student, you can access the classrooms, computer laboratories and cafeteria. However, you are prohibited from accessing the faculty room and server room. A faculty member can access more rooms compared to a student.

Mandatory Access Control (MAC)

MAC is the strictest type of access control. This access control can be seen in government especially in military. It uses Sensitivity Labels (SL) both for the subject (initiates an action) and object (waiting for action). It is also known as a multi-level type of access control.

SL can be classified as:

Top Secret Secret Confidential Public

Let's say a File A (Object) has an SL of Secret. Only the subject that has an SL of either Top Secret or Secret can access the file.

To visualize, let's say a 5-star General has an SL of Top Secret, Colonel with SL of Secret, Lieutenant with SL of Confidential and Sergeant with SL of Public. Only the Colonel or 5-Star General can access File A because they have clearance to do so because of their SL. A subject can access all objects that are below his/her SL. MAC uses a top-down approach.

Discretionary Access Control (DAC)

DAC is the direct opposite of MAC. In this case, this type of access control can be seen in non-military institutions (commercial use, usually). In DAC, the owner of the file determines the privilege of the subjects to the objects. It is also known as a single-level type of access control.

DAC uses an Access Control Matrix (r-read, w-write, x-execute) shown below:

S (down) O (right)	**Chicken File Owner: Riza Object 1**	**Pasta File Owner: Reese Object 2**	**Beef File Owner: Rex Object 3**
James Subject 1	rwx	---	-wx
Ray Subject 2	rw-	rw-	-wx
Ogawa Subject 3	---	rwx	-wx

In the above scenario, we have 3 users (subjects) trying to access 3 files (objects). Each file is owned by a specific individual (owner). It becomes the discretion of the owner on what privileges he/she wants to give the subjects. These privileges may change also.

Role-based Access Control (RBAC)

RBAC is also known as a non-discretionary access control. It gives privileges based on the roles/tasks. It is beneficial for large organizations in organizing group privileges to objects. For example, all students have read only access to File 1, File 2 and File 3. All faculty members, on the other hand, have full access to all the files mentioned. The admin will just add users (subjects) on the groups created for consistency and convenience.

Rule-based Access Control

Rule-based Access Control basically gives privilege based on a list of an enforced policy. A good example is an Access Control List (ACL) in a firewall. The firewall will grant/deny access based on the rules found in the ACL. However, if no rule is present, then no privilege should be given. (implicit deny)

----- NOTHING FOLLOWS -----