Authentication Mechanisms

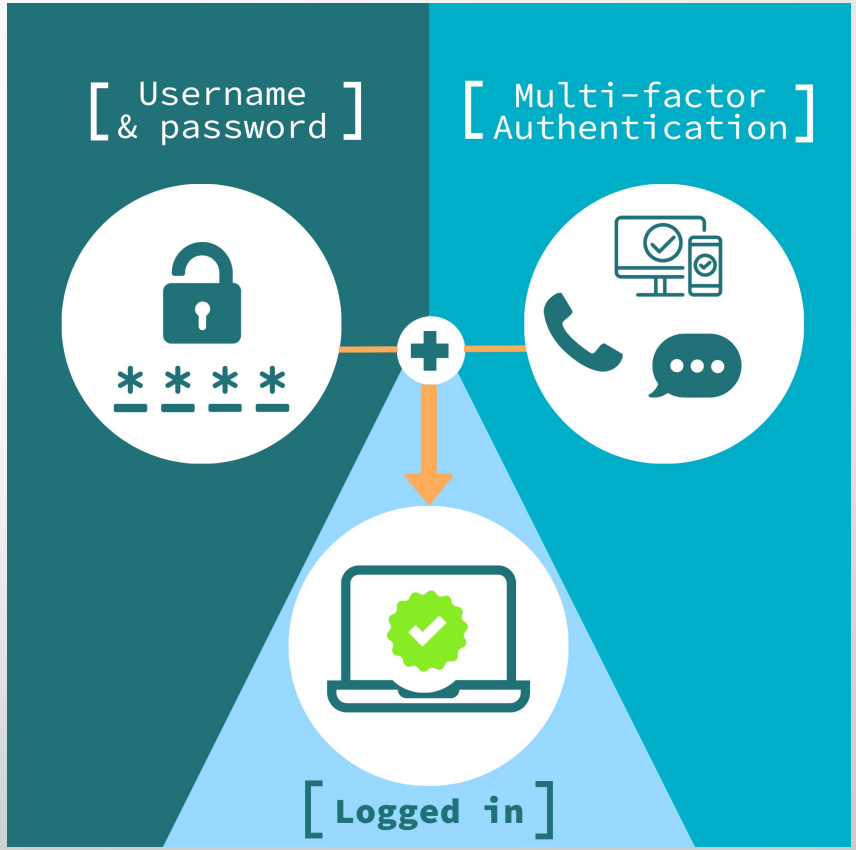
Dr Zia ur Rehman

Two Factor Authentication

- It is a security process that requires users to provide two different forms of identification in order to access an account or system.
- It is an additional layer of security that makes it more difficult for unauthorized individuals to gain access to sensitive information..
- 2FA can be something the user knows (such as a password or PIN) and something the user has (such as a smartphone or security token).
- When the user enters their password or PIN, they are then prompted to provide the second factor, such as a unique code sent to their phone or generated by a security token.

Two Factor Authentication

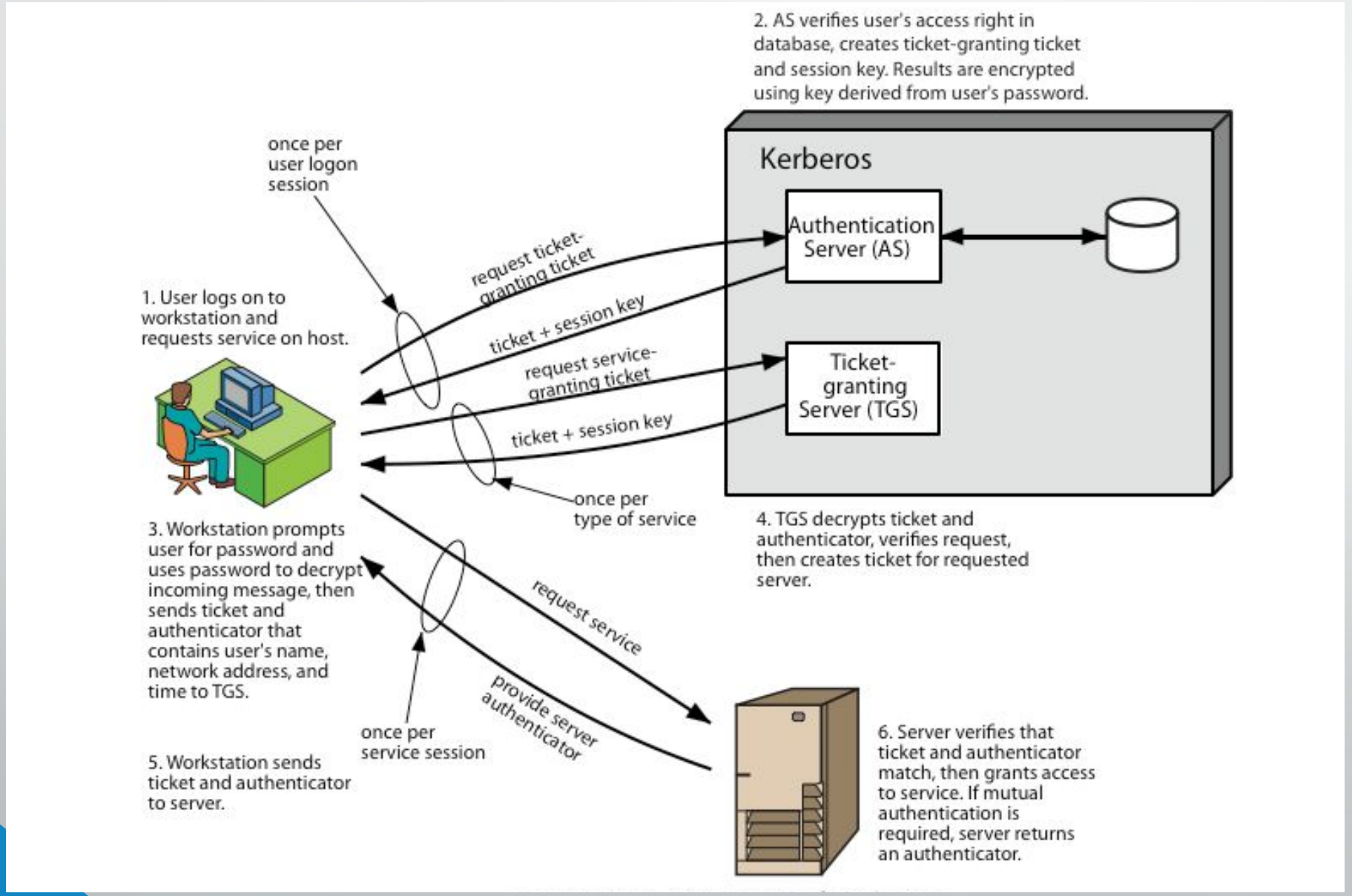
- There are several types of 2FAs:
  - SMS-based 2FA: A code is sent to the user's phone via SMS.
  - App-based 2FA: A code is generated by an app on the user's smartphone.
  - Hardware-based 2FA: A physical device, such as a security token, is used to generate a code.



Kerberos

- Trusted key server system from MIT
  - one of the best known and most widely implemented **trusted third party** key distribution systems.
- Provides centralised private-key third-party authentication in a distributed network
  - allows users access to services distributed through network
  - without needing to trust all workstations
  - rather all trust a central authentication server
- Two versions in use: 4 & 5

Kerberos 4 Overview



Kerberos Realms

- A Kerberos environment consists of:
  - a Kerberos server
  - a number of clients, all registered with server
  - application servers, sharing keys with server
- This is termed a realm
  - typically a single administrative domain
- If have multiple realms, their Kerberos servers must share keys and trust each other.

Access Control

- **Access control is the process of:**
  - identifying a person doing a specific job
  - authenticating them by looking at their identification
  - granting a person only the key to the door or computer that they need access to and nothing more.
- **In information security, one would look at this as:**
  - granting an individual permission to get onto a network via a username and password
  - allowing them access to files, computers, or other hardware or software they need
  - ensuring they have the right level of permission to do their job

Flavors of Access Control

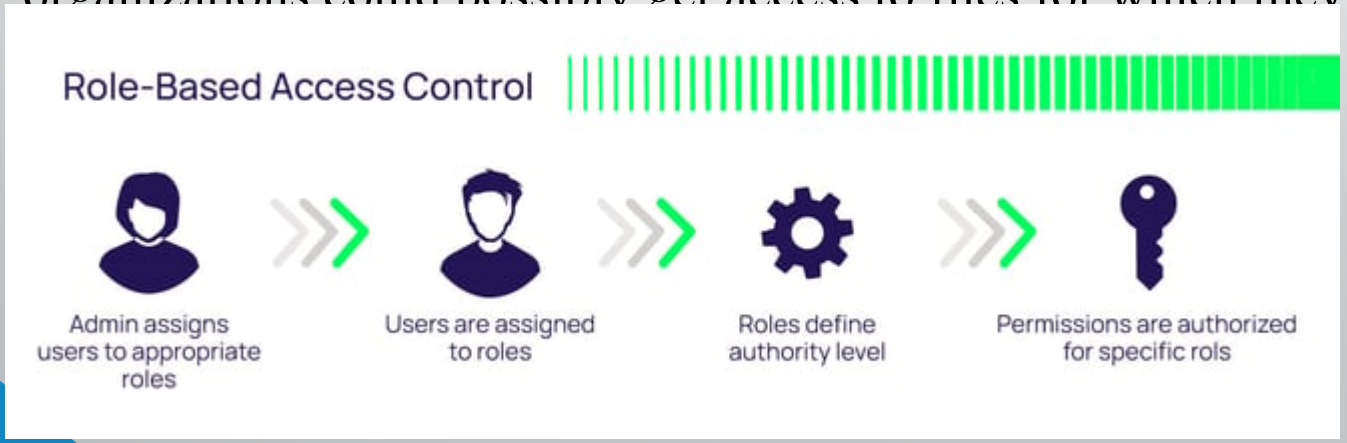
- Mandatory Access Control (MAC)
- Role-Based Access Control (RBAC)
- Discretionary Access Control (DAC)
- Rule-Based Access Control (RBAC or RB-RBAC)

MAC

- It gives access controls only to the owner and custodian management. This means the end user has no control over any settings that provide any privileges to anyone. Now, there are two security models associated with MAC: Biba and Bell-LaPadula.
- **Biba Model**:
  - focuses on integrity of information, Biba is a setup where a user with low-level clearance can read higher-level information (called “read up”) and a user with high-level clearance can write for lower levels of clearance (called “write down”).
  - The Biba model is typically utilized in businesses where employees at lower levels can read higher-level information and executives can write to inform the lower-level employees.
- **Bell-LaPadula Model**:
  - focuses on confidentiality of information. a setup where a user at a higher level (i.e. Top Secret) can only write at that level and no lower (called “write up”), but can also read at lower levels (called “read down”).
  - Bell-LaPadula was developed for governmental and/or military purposes where if one does not have the correct clearance level and does not need to know certain information, they have no business with the information.

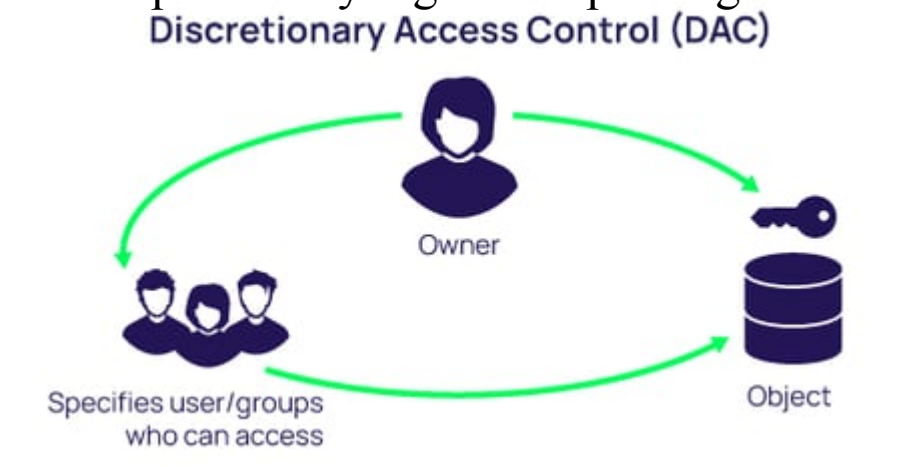
RBAC

- It provides access control based on the position an individual fills in an organization.
- So, instead of assigning Alice permissions as a security manager, the position of security manager already has permissions assigned to it. In essence, Alice would just need access to the security manager profile.
- **Big issue**:
  - If Alice requires access to other files, there has to be another way to do it since the roles are only associated with the position; otherwise, security managers from other organizations could possibly get access to files for which they are unauthorized.



DAC

- Model is the least restrictive model compared to the most restrictive MAC model. DAC allows an individual complete control over any objects they own along with the programs associated with those objects.
- Weaknesses:
  - First, it gives the end-user complete control to set security level settings for other users which could result in users having higher privileges than they're supposed to.
  - Secondly, and worse, the permissions that the end-user are inherited into other programs they execute. This means the end-user can execute malware without knowing it and the malware could take advantage of the potentially high-level privileges the end-user possesses.



Rule-Based Access Control

- Rule-Based Access Control will dynamically assign roles to users based on criteria defined by the custodian or system administrator.
- For example, if someone is only allowed access to files during certain hours of the day, Rule-Based Access Control would be the tool of choice.
- Rules may need to be “programmed” into the network by the custodian or system [illegible] the box.”