IAM (Identity and Access Management)

Identity Proofing

- Verification of personal information
- KBA
- Document Verification
- Biometric
- Use third-party services

SAML -> Authentication and Authorization (Federation when it in websites)
OAuth -> Only Authorization (don't share credentials)
OpenID -> Add Authentication to OAuth

Mandatory Access Control (MAC) -> Central authority based on different levels of security clearance, users can not change access permissions, they are set and enforced by administrator
LINUX SE

- Government
- Military

Discretionary Access Control (DAC) -> Resource owner decides on access levels (more flexible), this can be risk because users could grant excessive access
Windows + MAC + Common Linux

- Where users need control over the resource they own (setting file permissions on OS)

Role-Based Access Control (RBAC) -> Assign permissions based on user's role (assign permission to group and the group to the users)

- Corporate environments

Rule-Based Access Control (RuBAC) -> Permissions based on rules
FIREWALLS

Attribute-Based Access Control (ABAC) -> Uses policies that evaluate attributes (more granular)
NETFLIX

- Complex environments with divers and dynamic users
- Attributes:
  - Screen size

- Localization
- Age