ACCESS CONTROL

Presented by :

Haider Shamil

Jwan Jamal

Supervised by :

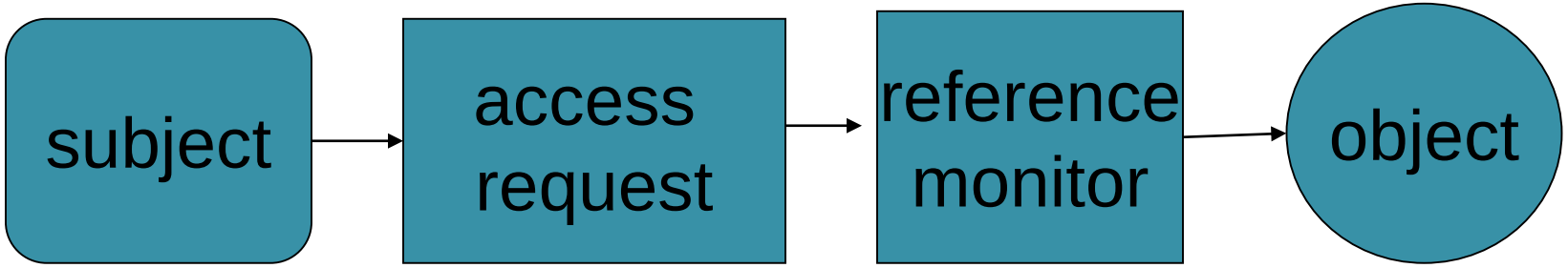
Dr.Bashar M.Nema

OUTLINE :-

- What is Access control
- security principle of control access.
- Access control models
- Types of Access Controls
- Access Control Techniques
- Threats to Access Control
- Categories of Access Controls
- Summary
- References

What is Access control

- Access Controls: The security features that control how users and systems communicate and interact with one another.
- Access control is the heart of Information Security!
- Access: The flow of information between subject and object
- Subject: An active entity that requests access to an object or the data in an object
- Object: A passive entity that contains information



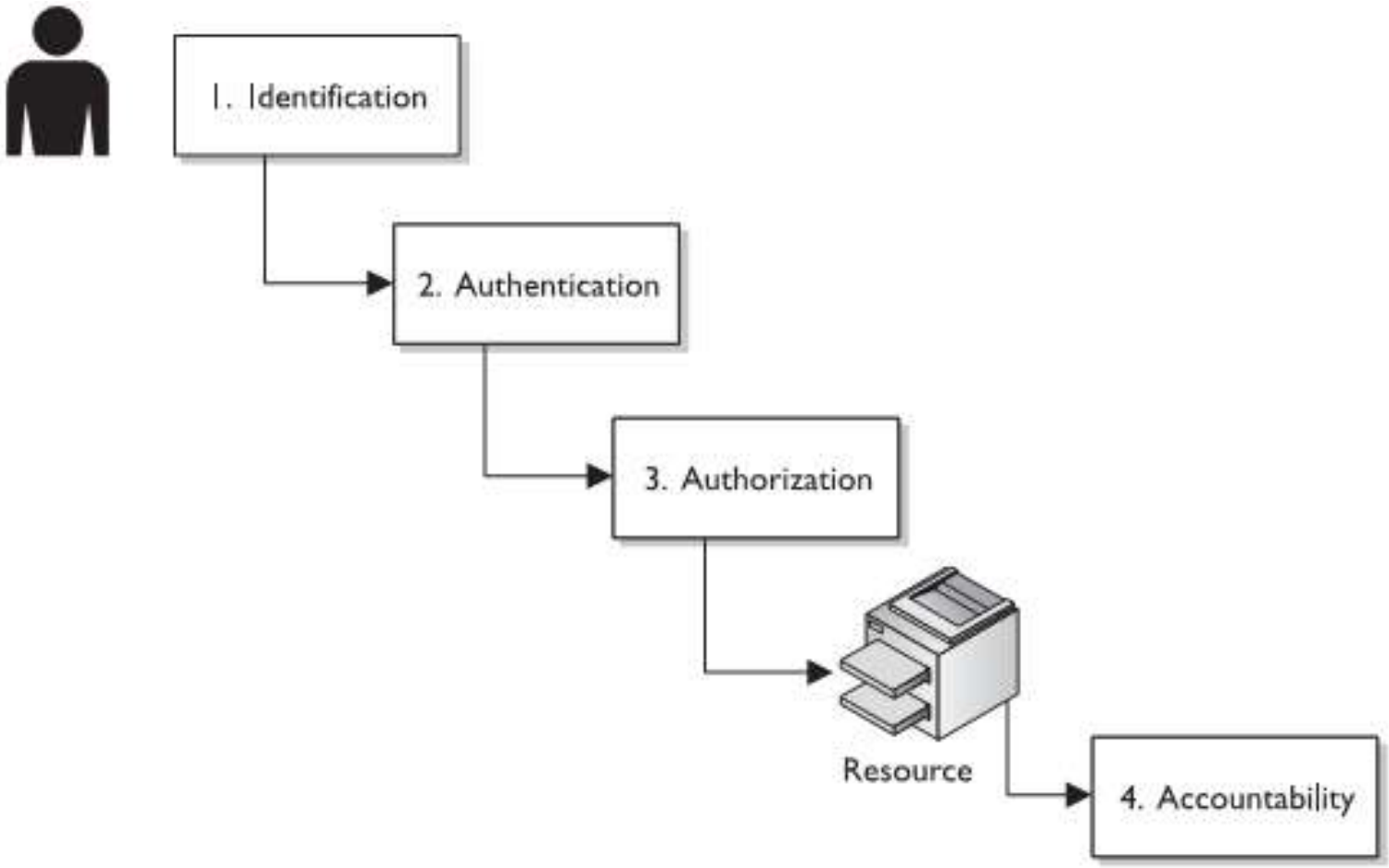
source (e.g. users, processes)

request

guard

resource (e.g. files, printers)

Security principle of control access



protect from un-authorized access

Identification

- Method of establishing the subject's identity
  - –User, Program, Process
  - –Use of username or other public information
- Identification component requirements…
  - –Each value should be unique
  - –Follow a standard naming scheme
  - –Non-descriptive of the user's position or tasks
  - –Must not be shared between users

Authentication

- Method of proving the identity
- How to prove an identity
  - –Use of passwords, token, or biometrics other private information
  - –Strong authentication is important

Authorization

- Determines that the proven identity has some set of characteristics associated with it that gives it the right to access the requested resources

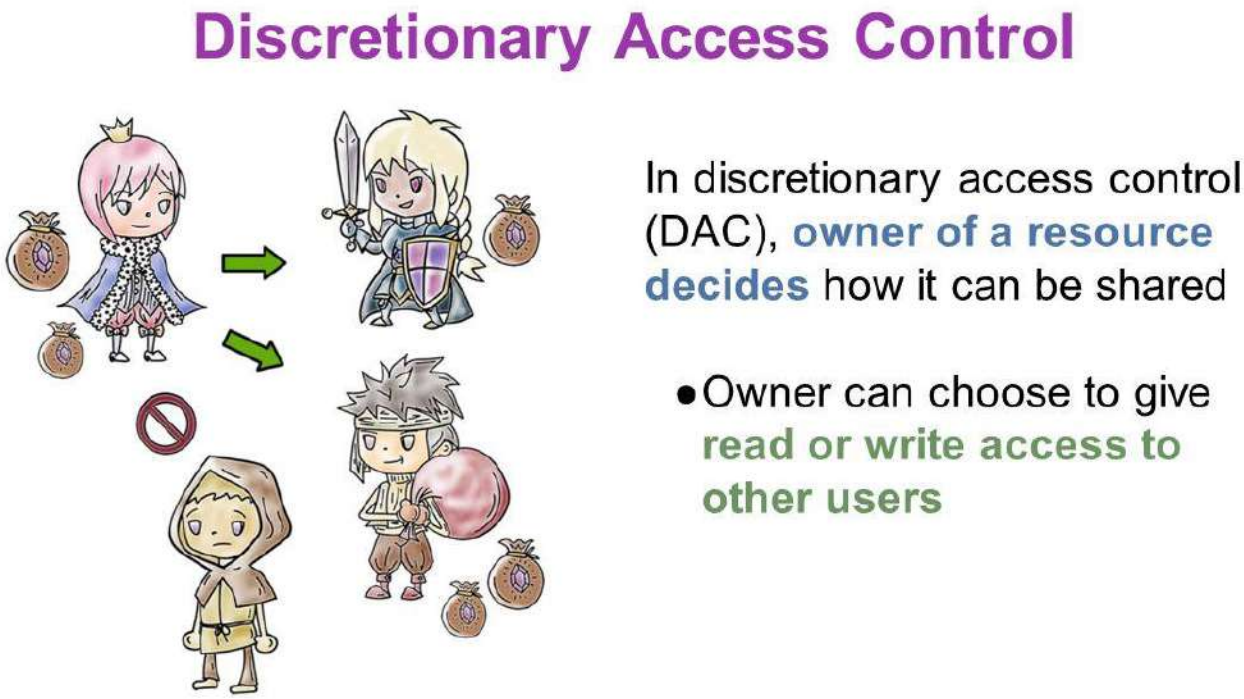
Accountability

- Audit log and monitoring to track subject activities with objects.
- Goal is to protect from un-authorized access

Access control models

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Non-Discretionary (Role Based) Access Control Models (RBAC)
- OTHER…

- Discretionary Access Control (DAC)
  - A system that uses discretionary access control allows the owner of the resource to specify which subjects can access which resources.
  - Access control is at the discretion of the owner.

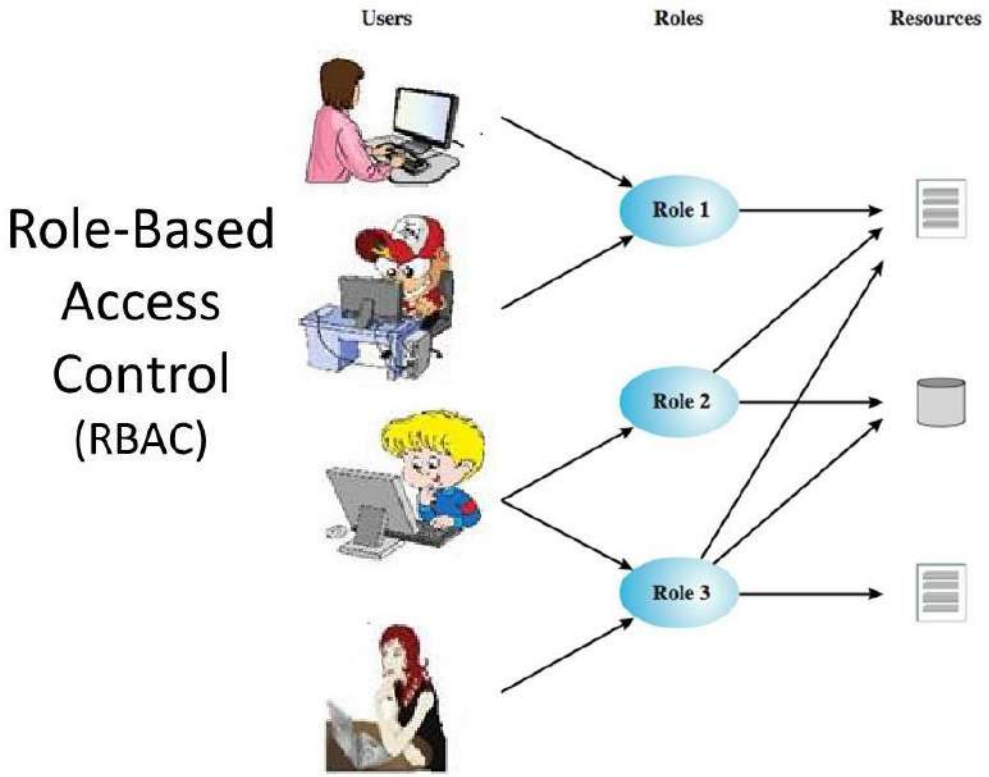


- Mandatory Access Control (MAC)
  - Access control is based on a security labeling system. Users have security clearances and resources have security labels that contain data classifications.
  - This model is used in environments where information classification and confidentiality is very important (e.g., the military).

Mandatory Access Control (MAC) Models

- User works in a company and the company decides how data should be shared
  - Hospital owns patient records and limits their sharing
    - Regulatory requirements may limit sharing

- Non-Discretionary (Role Based) Access Control Models
  - Role Based Access Control (RBAC) uses a centrally administered set of controls to determine how subjects and objects interact.
  - Is the best system for an organization that has high turnover.



Traditional Access Control Models

	Advantage	Disadvantage
DAC	• Easy to implement • Highly flexible	• Doesn't scale well • ACL explosion possibility • Prone to mistakes
MAC	• Most secure • Easy to scale	• Not flexible • Limited user Functionality • High admin overhead
RBAC	• Scalable • Flexible – user & permission • are loosely coupled • Less administration required	• Roles needs provisioning and maintenance • Possibility of role explosion • Unable to accommodate realtime context

Types of Access Controls

- There are three types of Access Controls:
- Administrative controls

  Define roles, responsibilities, policies, and administrative functions to manage the control environment.
- Technical controls

  Use hardware and software technology to implement access control.
- Physical controls

  Ensure safety and security of the physical environment

Administrative Controls

- Ensure that technical and physical controls are understood and properly implemented

–Policies and procedures

–Security awareness training

–Asset classification and control

–Account administration

–Account, log monitoring

Technical Controls

- Examples of Technical Controls are:
  - Encryption
  - Smart cards
  - Access control lists
  - Violation reports
  - Network monitoring and intrusion detection

Physical Controls

- Examples of Physical Controls are:
  - Fences, locked doors, and restricted areas
  - Guards
  - Motion detectors
  - Video cameras
  - Fire detectors

Access Control Techniques

- Constrained User Interfaces
- Access Control Matrix
- Content Dependent Access Control
- Context Dependent Access Control

Access Control Techniques

- Constrained User Interfaces
  - Restrict user's access abilities by not allowing them certain types of access, or the ability to request certain functions or information
- Access Control Matrix
  - Is a table of subjects and objects indicating what actions individual subjects can take upon individual objects.

Access Control Techniques

- Content Dependent Access Control
  - Access to an object is determined by the content within the object.
- Context Dependent Access Control
  - Makes access decision based on the context of a collection of information rather than content within an object.

Threats to Access Control

- A few threats to access control
  - Insiders
    - Countermeasures include good policies and procedures, separation of duties, job rotation
  - Dictionary Attacks
    - Countermeasures include strong password policies, strong authentication, intrusion detection and prevention
  - Brute Force Attacks
    - Countermeasures include penetration testing, minimum necessary information provided, monitoring, intrusion detection, clipping levels
  - Spoofing at Logon
    - Countermeasures include a guaranteed trusted path, security awareness to be aware of phishing scams, SSL connection

Categories of Access Controls

Control Type	Description
Preventative	Keep undesirable events from Happening
Detective	Identify undesirable events that have taken place
Corrective	Correct undesirable events that have taken place
Deterrent	Discourage security violations from taking place
Recovery	Restore resources and capabilities after a violation or accident
Compensation	Provide alternatives to other Controls

Summary

- What is Access control
  - Access Controls
  - Access
  - Subject
  -object
- security principle of control access.
  - Identification
  - authentication
  - Authorization
  - Accountability
- Access control models
  -Discretionary Access Control(DAC)
  -Mandatory Access Control (MAC)
  -Non-Discretionary (Role Based) Access Control Models(RBAC)
- Types of Access Controls
  -Administrative controls
  -Technical controls
  -Physical controls
- Access Control Techniques
  -Constrained User Interfaces
  -Access Control Matrix
  -Content Dependent Access Control
  -Context Dependent Access Control.
- Threats to Access Control
  -Insiders
  -Dictionary Attacks
  -Brute Force Attacks
  -Spoofing at Logon.
- Categories of Access Controls

References

- ”Xin Jin”,”Ram Krishnan”, ”Ravi Sandhu”,” A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC”,”2012”.
- “D.R. Kuhn”, “E.J. Coyne”,” T.R. Weil”,” Adding Attributes to Role Based Access Control”, “IEEE Computer,” “2010”).
- “Park, J., Nguyen”,“ Sandhu”, “R. A provenance-based access control model”. “Privacy, Security and Trust (PST)” “2012” .
- “william stallings “,“lawrie brown”,” computer security principles and practice”,” ACM/IEEE Computer Science Curricula”, “2013”.