Chapter 4:
ACCESS CONTROL, AUTHORIZATION AND AUTHENTICATION

Access Control, Authorization

- Definitions
- Access Rights
- Access Control Systems
- Authorization
- Types of Authorization Systems
- Authorization Principles
- Authorization Granularity
- Web Access and Authorization

Definitions

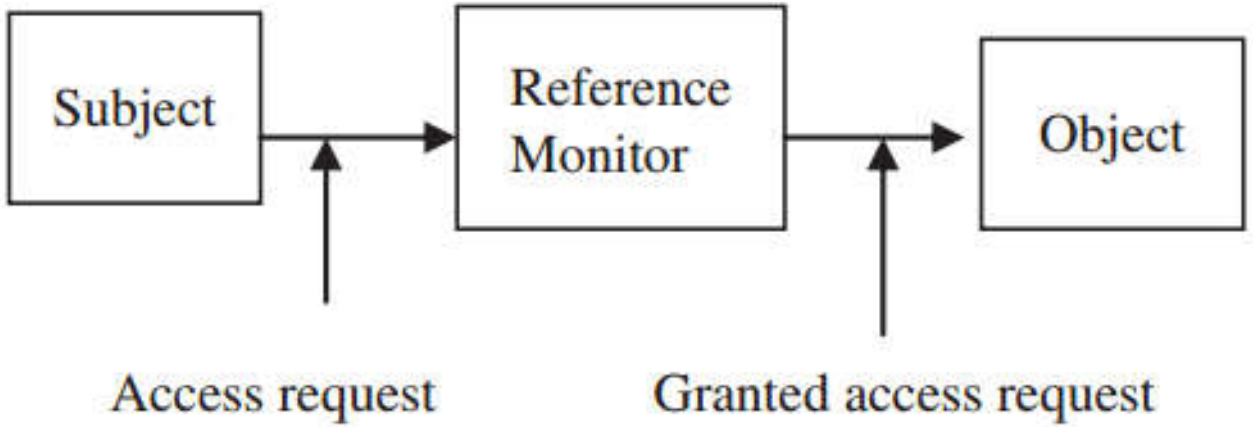
- Access control is a process to determine “Who does what to what,” based on a policy.
- Access control is one of the major cornerstones of system security

Access Control, Authorization

- Definitions
- Access Rights
- Access Control Systems
- Authorization
- Types of Authorization Systems
- Authorization Principles
- Authorization Granularity
- Web Access and Authorization

Access Rights

- Access control consists of four elements: subjects, objects, operations, and a reference monitor.
  - Subjects are system users and groups of users
  - Objects are files and resources such as memory, printers, and scanners including computers in a network.
  - An access operation comes in many forms including Web access, server access, memory access, and method calls
- Access Control List(ACL)



Access Rights

- Whenever a subject requests to access an object, an access mode must be specified:
  - Observe: subject may only look at the content of the object
  - Alter: the subject may change the content of the object

Access Rights

- Access rights refer to the user's ability to access a system resource. There are four access rights: execute, read, append, and write.

	execute	append	read	write
observe			X	X
alter		X		X

- Access rights and access modes are different

Access Rights

- Access rights can be set individually on each system resource for each individual user and group.
- User can belong to many groups and enjoy those groups' rights.
- User access rights and group access rights

Access Rights

Access Control Techniques and Technologies:

- Several control techniques and technologies:
  - access control matrix
  - capability tables
  - access control lists
  - role-based access control
  - rule-based access control
  - restricted interfaces
  - content-dependent access control.

Access Rights

Access Control Techniques and Technologies:

- Access control matrix:

Objects → Subjects/groups ↓	R1	R2	R3	R4
A	W	R	R	W
B	R			
Group G1	W			
Group G2		W		
C				R

Access Rights

Access Control Techniques and Technologies:

- Access control list:

Object	Access rights	Subjects
R1	W	A
	R	B
	W	Group G1
R2	R	A
	W	Group G2
R3	R	A
R4	R	A
	R	C

Access Rights

Access Control Techniques and Technologies:

- Capability tables:

Subject	Object 1/Access	Object 2/Access	Object 3 /Access	Object 4/Access
A	R1/W	R2/R	R3/R	R4/R
B	R1/R			
Group G1	R1/W			
Group G2		R2/W		
C				R4/R

Access Rights

Access Control Techniques and Technologies:

- Role-based access control:
  - System security in role-based access control (RBAC) is based on roles assigned to each user in an organization. For ex, a user may be assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role.

Access Rights

Access Control Techniques and Technologies:

- Rule-based access control(RBAC), also known as policy-based access control(PBAC), is based on the least privileged concept.
- RBAC is a multipart process, where one process assigns roles to users just like in the role-based access control techniques discussed above.
- The second process assigns privileges to the assigned roles based on a predefined policy.
- Another process is used to identify and authenticate the users allowed to access the resources.

Access Rights

Access Control Techniques and Technologies:

- Restricted Interfaces:

- To get access to restricted data, the user has to go via an interface,
- Any outside party access to restricted data requires a special access request, which many times requires filling in an online form.
- The interfaces restrict the amount and quality of data that can be retrieved based on filter and retrieval rules

Access Control, Authorization

- Definitions
- Access Rights
- Access Control Systems
- Authorization
- Types of Authorization Systems
- Authorization Principles
- Authorization Granularity
- Web Access and Authorization

Access Control Systems

- Physical Access Control
- Access Cards: magnetic , smart cards, …
- Biometrics
- ……

Access Control, Authorization

- Definitions
- Access Rights
- Access Control Systems
- Authorization
- Types of Authorization Systems
- Authorization Principles
- Authorization Granularity
- Web Access and Authorization

Authorization

- Authorization is the determination of whether a user has permission to access, read, modify, insert, or delete certain data, or to execute certain programs
- Authorization is also commonly referred to as access permissions, and it determines the privileges a user has on a system and what the user should be allowed to do to the resource.
- Access permissions are normally specified by a list of possibilities
- For example, UNIX allows the list {read, write, execute} as the list of possibilities for a user or group of users on a UNIX file

Authorization

- Authorization Mechanisms: two main categories: discretionary and mandatory
  - Discretionary Authorization: allow subjects to grant other users authorization to access the data.
  - Mandatory Access Control: prevent any illegal flow of information through the enforcement of multilevel security by classifying the data and users into various security classes

Authorization

- Types of Authorization Systems:
  - Centralized
  - Decentralized
  - Implicit
  - Explicit

Authorization

- Authorization Principles:
  - Least Privileges: the subject be granted authorizations based on its needs.
  - Separation of duties: breaks down the process of authorization into basic steps and requires that for every request for authorization from a subject to a system resource, each step be given different privileges

Authentication

- Definition
- Authentication elementents
- Types of Authentication
- Authentication Methods

Definition

- Authentication is the process of validating the identity of someone or something.
- Generally, authentication requires the presentation of credentials or items of value to really prove the claim of who you are. The items of value or credential are based on several unique factors that show:
  - Something you know: passwords, PINs
  - Something you have: cards, tags
  - Something you are: fingerprints, retinal patterns, DNA patterns, and hand geometry
  - Somewhere you are

Definition

- Authentication takes one of the following three forms:
  - Basic authentication.
  - Challenge-response.
  - Centralized authentication.
- Multiple factors and effectiveness of authentication:
  - Systems using two or more methods can result in greater system security.
  - To combine two or more authentication items from two or more factors (possible to combine two or more items from the same authentication factor class)

Authentication elementents

- An authentication process is based on five different elements:
  - The person or group of people seeking authentication
  - Distinguishing characteristics from that person or group presented for authentication.
  - The authenticator: user-designated server, a virtual private network (VPN), firewall, a local area network (LAN) server, independent authentication service, …
  - The authenticating mechanism: to verify the presence of the authenticating characteristics
  - The access control mechanism: to accept or deny authentication.

Types of Authentication

Table 10.1 Authentication factors and their vulnerabilities[1]

Number	Factor	Examples	Vulnerabilities
1	What you know	Password, PIN	Can be forgotten, guessed, duplicated
2	What you have	Token, ID Card, Keys	Can be lost, stolen, duplicated
3	What you are	Iris, voiceprint, fingerprint	Nonrepudiable

[1]Ratha, Nalini K., Jonathan H. Connell and Ruud M. Bolle. "Secure Fingerprint-based Authentication for Lotus Notes." http://www.research.ibm.com/ecvg/pubs/ratha-notes.pdf.

- Two types:
  - Nonrepudiable authentication
  - Repudiable authentication

Types of Authentication

- Nonrepudiable authentication:
  - all items in factor 3 (what you're): iris patterns, retinal images, and hand geometry,…
  - biometric characteristics cannot be forgotten, lost, stolen, guessed, or modified by an intruder.
  - biometrics as nonrepudiable authentication items are undeniable.

Types of Authentication

- Repudiable authentication:
  - The first two factors, “what you know” and “what you have,” can be unreliable.
  - Can be lost, forged, or easily duplicated

Authentication Methods

- Different authentication methods are used based on different authentication algorithms
- Authentication methods can be combined or used separately, depending on the level of functionality and security needed
  - password authentication
  - public-key authentication
  - anonymous authentication
  - remote authentication
  - certificate-based authentication

Authentication Methods

- Password authentication:
  - Reusable Passwords: user authentication & client authentication (establishes users' identities and controlled access to system resources) -> the most widely used authentication methods but unreliable.
  - One-time password authentication (session authentication): S/Key password & Token password
  - Challenge-Response Passwords
  - Combined Approach Authentication

Authentication Methods

- Public-key authentication:
  - The centralized authentication server, commonly known as the access control server(ACS), uses public key systems.
    - When a user tries to access an ACS, it looks up the user's public keys and uses it to send a challenge to the user.
    - The server expects a response to the challenge where the user must use his or her private key.
    - If the user then signs the response using his or her private key, he or she is authenticated as legitimate.
  - The ACS is used in several authentication schemes including SSL, Kerberos, and MD5 authentication.

Reference

- Guide to Computer Network Security
  - Chapter 09: pg 185 – 203
  - Chapter 10: pg 207 - 223