Access Control

Dr. Talal Alkharobi

Access control

- The ability to permit or deny the use of something by someone.
- In physical security, refers to the practice of restricting entrance to a property, a building, or a room to authorized persons.
- Physical access control can be achieved by
  - human (a guard, bouncer, or receptionist),
  - mechanical means such as locks and keys, or
  - technological means such as a card access system.

3

Access Control

- Also includes measures such as
  - physical devices,
  - biometric locks,
  - hidden paths,
  - digital signatures,
  - encryption,
  - social barriers,
  - monitoring by humans and
  - Monitoring by automated systems.

4

Access Control Model

- Subject: the entitie that can perform actions in the system
- Object: the entitie representing resources to which access may need to be controlled
- Subjects and objects should both be considered as software entities, rather than as human users.
- Human user can only have an effect on the system via the software entities that they control.
- Some systems equate subjects with user IDs, so that all processes started by a user by default have the same authority
- In some models any software entity can potentially act as both a subject and object

5

Access Control

- Access control models used by current systems tend to fall into one of two classes:
  - based on capabilities
  - based on access control lists (ACLs).
- Both capability-based and ACL-based models have mechanisms to allow access rights to be granted to all members of a group of subjects (often the group is itself modeled as a subject).

6

Capability-Based model

- Holding an unforgeable reference or capability to an object provides access to the object
- Possession of a house key grants the access to the house
- Access is conveyed to another party by transmitting such a capability over a secure channel.

7

ACL-based model

- A subject's access to an object depends on whether its identity is on a list associated with the object
- A bouncer at a private party would check your ID to see if your name is on the guest list
- Access is conveyed by editing the list.
- Different ACL systems have a variety of different conventions regarding who or what is responsible for editing the list and how it is edited

Dr. Talal Alkharobi

8

Access Control

- Access control systems provide the essential services of
  - Identification
  - Authentication
  - Authorization,
  - Accountability

Dr. Talal Alkharobi

9

Identification

- Identification is how a user tells a system who he or she is (username).
- The identification component of an access control system is normally a relatively simple mechanism based on either Username or User ID.
- In the case of a system or process, identification is usually based on:
  - Computer name
  - Media Access Control (MAC) address
  - Internet Protocol (IP) address
  - Process ID (PID)

Dr. Talal Alkharobi

10

Identification requirements

- Must uniquely identify the user.
- Shouldn't identify that user's position or relative importance in an organization (such as labels like president or CEO).
- Should avoid using common or shared user accounts, such as root, admin, and sysadmin.
- Such accounts provide no accountability and are juicy targets for hackers.

Dr. Talal Alkharobi

11

Authentication

- The act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the thing are true.
- Authenticating an object may mean confirming its provenance
- Authenticating a person often consists of verifying their identity

Dr. Talal Alkharobi

12

Authentication

- The process of verifying a user's claimed identity
- For example, by comparing an entered password to the password stored on a system for a given username

Dr. Talal Alkharobi

13

Authentication factors

- Something you know
- Something you have
- Something you are

- Authentication depends upon one or more factors.

14

Authentication Something you know

- As a password or a personal identification number (PIN).
- This assumes that only the owner of the account knows the password or PIN needed to access the account.

15

Authentication
Something you have

- Such as a smart card or token.
- This assumes that only the owner of the account has the necessary smart card or token needed to unlock the account.

Dr. Talal Alkharobi

16

Authentication
Something you are

- Fingerprint,
- Voice,
- Retina,
- Iris characteristics

Dr. Talal Alkharobi

17

Authentication

- In computer security, authentication is the process of attempting to verify the digital identity of the sender of a communication such as a request to log in.
- In a web of trust, "authentication" is a way to ensure users are who they say they are—that the user who attempts to perform functions in a system is in fact the user who is authorized to do so.

Dr. Talal Alkharobi

18

Authentication

- The sender being authenticated may be
  - person using a computer
  - computer itself
  - computer program

Dr. Talal Alkharobi

19

Strong authentication

- Layered authentication approach relying on more than one authenticators to establish the identity of an originator or receiver of information.

20

eAuthentication

- Defined in 2003 as the Web Based service that provides authentication to end users accessing (logging into) an Internet service.
- The eAuthentication is similar to Credit Card verification for eCommerce web sites.
- The verification is done by a dedicated service that receives the input and returns success or fail indication.

21

eAuthentication Example

- An end user wishes to enter his eBuy or eTrade web site.
- He gets the Login web page and is required to enter his user ID and a Password
- The information is transmitted to the eAuthentication service as a query.
- If the service returns Success – the end user is permitted into the eTrade service with his privileges as a user.

22

authorization

- The process to decide if person, program or device is allowed to have access to data, functionality or service.
- When a consumer tries to use a resource, the authorization process checks that the consumer has been granted permission to use that resource.

23

Authorization

- consumers
  - computer users,
  - computer programs
  - devices on the computer.

Dr. Talal Alkharobi

24

Authorization

- Resources
  - individual files or items data,
  - computer programs,
  - computer devices
  - functionality provided by computer applications.

Dr. Talal Alkharobi

25

Authorization

- Authorization applies to resources rather than to consumers
- The association between a consumers and resources initially controlled by that user having been determined by Identification and authentication

26

Authorization

- These rights and permissions are implemented differently based on either
  - discretionary access control (DAC)
  - mandatory access control (MAC)

27

authorization

- Permissions are generally defined by the computer's system administrator in some types of "security policy application“ such as access control list or a capability, on the basis of the "principle of least privilege"
- Principle of least privilege: consumers should only be granted permissions they need to do their jobs.

Dr. Talal Alkharobi

28

authorization

- "Anonymous consumers" or "guests", are consumers that have not been required to authenticate.
- They often have very few permissions.

Dr. Talal Alkharobi

29

authorization

- Some security policy applications, by default, grant full access to all consumers to all resources.
- Others do the opposite, insisting to takes deliberate action to enable a consumer to use each resource.

Dr. Talal Alkharobi

30

OS Authorization

- Most modern, multi-user operating systems include an authorization process.
- Authorization is part of the operating system that protects computer resources by only allowing those resources to be used by consumers that have been granted authority to use them.
- Older and single user operating systems often had weak or non-existent authentication and authorization systems.

Dr. Talal Alkharobi

31

OS Authorization

- OS define sets of permissions that are variations or extensions of three basic types of access:
  - Read (R): The subject can
    - Read file contents
    - List directory contents
  - Write (W): The subject can change the contents of a file or directory with these tasks:
    - Add
    - Create
    - Delete
    - Rename

32

OS Authorization

- Execute (X): If the file is a program, the subject can cause the program to be run. (In Unix systems, the 'execute' permission doubles as a 'traverse directory' permission when granted for a directory.)

33

Authentication vs. Authorization

- The problem of authorization is often thought to be identical to that of authentication;
- Authentication: the process of verifying a person's identity
- Authorization: the process of verifying that a known person has the authority to perform a certain operation.
- Authentication, therefore, must precede authorization.

Dr. Talal Alkharobi

34

Authentication vs. Authorization

- When you show proper identification to a bank teller, you could be authenticated by the teller, and you would be authorized to access information about your bank accounts. You would not be authorized to access accounts that are not your own.
- Since authorization cannot occur without authentication, the former term is sometimes used to mean the combination of authentication and authorization.

Dr. Talal Alkharobi

35

Accountability

- It is a concept in ethics with several meanings like
  - answerability,
  - responsibility,
  - blameworthiness,
  - liability

Dr. Talal Alkharobi

36

Accountability

- A system components to associate a subject with its actions. (as audit trails (records) and logs)
- The information recorded should be sufficient to map the subject to a controlling user.
- Audit trails and logs are important for
  - Detecting security violations
  - Re-creating security incidents

Dr. Talal Alkharobi

37

Accountability

- If no one is regularly reviewing the logs and they are not maintained in a secure and consistent manner, they may not be admissible as evidence.

38

Accountability

- Many systems can generate automated reports based on certain predefined criteria or thresholds, known as clipping levels.
- These reports help a system administrator or security administrator to more easily identify possible break-in attempts.

39

Accountability

- For example, a clipping level may be set to generate a report for the following:
  - More than three failed logon attempts in a given period
  - Any attempt to use a disabled user account

40

Access Control Techniques

- Discretionary Access Control
- Mandatory Access Control

41

Discretionary access control (DAC)

- Means of restricting access to objects based on the identity and need-to-know of users and/or groups to which the object belongs.
- Controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (directly or indirectly) to any other subject.

42

Discretionary access control (DAC)

- Occasionally a system as a whole is said to have "discretionary" or "purely discretionary" access control as a way of saying that the system lacks mandatory access control.
- On the other hand, systems can be said to implement both MAC and DAC simultaneously, where DAC refers to one category of access controls that subjects can transfer among each other and MAC refers to a second category of access controls that imposes constraints upon the first.

Discretionary Access Control

43

- Two important concepts in DAC are
  - File and data ownership: Every object in the system has an owner. In most DAC systems, each object's initial owner is the subject that caused it to be created. The access policy for an object is determined by its owner.
  - Access rights and permissions: These are the controls that an owner can assign to other subjects for specific resources.

Mandatory Access Control (MAC)

44

- An access policy determined by the system, not the owner.
- MAC is used in multilevel systems that process highly sensitive data, such as classified government and military information.
- A multilevel system is a single computer system that handles multiple classification levels between subjects and objects.
- Few systems implement MAC (XTS-400)

45

Mandatory Access Control Sensitivity labels

- In a MAC-based system, all subjects and objects must have labels assigned to them.
- A subject's sensitivity label specifies its level of trust.
- An object's sensitivity label specifies the level of trust required for access.
- In order to access a given object, the subject must have a sensitivity level equal to or higher than the requested object.

46

Mandatory Access Control Data import and export

- Controlling the import of information from other systems and export to other systems (including printers) is a critical function of MAC-based systems, which must ensure that sensitivity labels are properly maintained and implemented so that sensitive information is appropriately protected at all times.

47

Mandatory Access Control

- Two methods are commonly used for applying MAC
  - Rule-based access controls:
  - Lattice-based access controls

48

Rule-based access controls

- This type of control further defines specific conditions for access to a requested object.
- All MAC-based systems implement a simple form of rule-based access control to determine whether access should be granted or denied by matching:
  - An object's sensitivity label
  - A subject's sensitivity label

Lattice-based access controls

49

- These can be used for complex access control decisions involving multiple objects and/or subjects.
- A lattice model is a mathematical structure that defines greatest lower-bound and least upper-bound values for a pair of elements, such as a subject and an object.

Access Control other definitions

50

- A service feature or technique used to permit or deny use of the components of a communication system.
- A technique used to define or restrict the rights of individuals or application programs to obtain data from, or place data onto, a storage device.
- The definition or restriction of the rights of individuals or application programs to obtain data from, or place data into, a storage device.
- The process of limiting access to the resources to authorized users, programs, processes, or other systems.

51

Access Control other definitions

- That function performed by the resource controller that allocates system resources to satisfy user requests.

52

Public Policy

- Access control to restrict access to systems ("authorization") or to track or monitor behavior within systems ("accountability") is an implementation feature of using trusted systems for security or social control.