İTÜ
Computer Security

Access Control

Dr. Şerif Bahtiyar
bahtiyars@itu.edu.tr

1

Before Starting

Russian Hacking Attacks Could 'Flood Us Cities With Sewage' And Cause Deadly Explosions

https://www.independent.co.uk/life-style/gadgets-and-tech/news/russian-hacking-attacks-us-power-grid-sewage-explosions-a8462691.html

2

Before Starting

Yaşanan Erişim Sorunu Hakkında Bilgilendirme:

Garanti BBVA

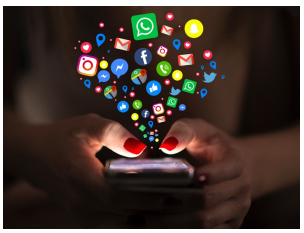
Dijital kanallarımızdaki hizmetlere erişimin yavaşlatılması ya da engellenmesine yönelik, DDOS (Distributed Denial of Service, Dağıtık Hizmet Engelleme) olarak adlandırılan bir atak mevcuttur.

https://www.garantibbva.com.tr/tr/garanti_hakkinda/garantiden_haberler/2019/ekim/dijital-kanallarimizdaki-hizmetlere-erisim.page

3

Before Starting

Stalkerware: The software that spies on your partner



Amy says it all started when her husband seemed to know intimate details about her friends.

https://www.bbc.com/news/technology-50166147

4

Outline

- Definition of Access Control
- Access Control Functions, Policies, and Requirements
- Elements of Access Control
- Discretionary Access Control
- Role-Based Access Control
- Attribute-Based Access Control
- Other Access Control Models
- Identity, Credential, and Access Management
- Trust Frameworks

5

Definition of Access Control

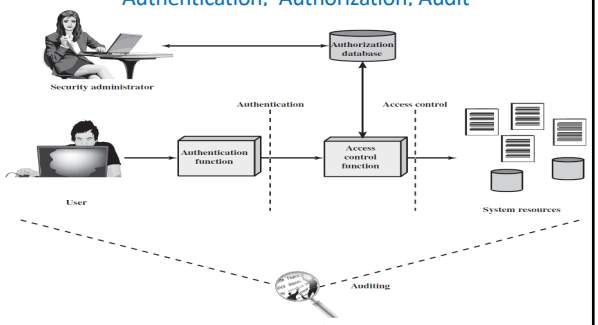
- Access Control: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

- Central element of computer security
- We consider user groups, not networked environment.
- All systems need access control.
- Access control mechanisms mediate between a user and system resources.

6

Access Control Functions

Authentication, Authorization, Audit



7

Access Control Policies

Discretionary Access Control (DAC)

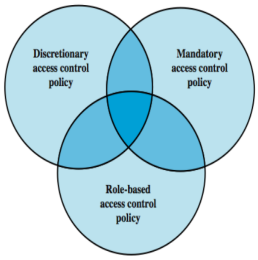
- Access based on the identity of the requestor and on access rules
- An entity may enable another entity to access resources

Mandatory Access Control (MAC)

- Access based on comparing security labels
- An entity cannot enable another entity to access resources

Role-Based Access Control (RBAC)

- Access based on roles of users



8

Access Control Policies

Attribute-Based Access Control (ABAC)

Access based on attributes of the user, the resource to be accessed, and current environmental conditions

In Application Security

- Authorization policies and attributes are defined in a technology neutral way.
- Policies for one API can be reused for another API
- Common application benefit from ABAC (Wikipedia)
  - Content management systems
  - Home grown applications
  - WEB APPLICATIONs

9

Access Control Requirements

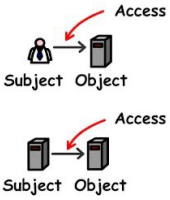
- Reliable input (authentication)
- Fine and coarse specifications
- Least privilege
- Separation of duty
- Open and closed policies
- Policy combinations, conflict resolution
- Administrative policies
- Dual control

10

Elements of Access Control

Subject: is an entity capable of accessing objects.

- A process representing user or application
- Often have three classes: owner, group, world

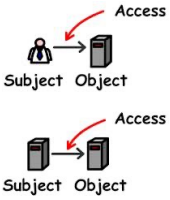


11

Elements of Access Control

Object: a resource to which access is controlled.

- Files, records, directories, programs, …
- Number and type depend on environment

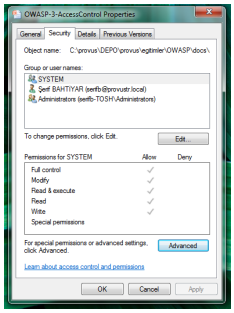


12

Elements of Access Control

Access right: describes the way in which a subject may access an object.

- Read, write, execute, delete, search, create



13

Discretionary Access Control (DAC)

Generally provided with access control matrix

- lists subjects in one dimension (rows)
- lists objects in the other dimension (columns)
- each entry specifies access rights of the specified subject to object
- is often sparse

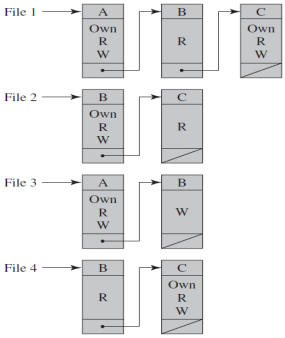
		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

14

Discretionary Access Control (DAC)

Access control list (ACL)

- Matrix decomposition by columns
- Convenient from subject side
- Inconvenient for determining access rights to a specific user

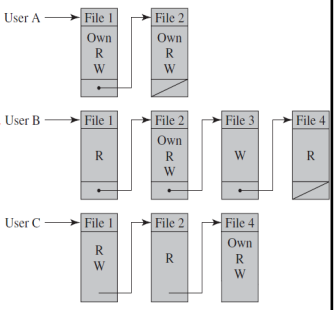


15

Discretionary Access Control (DAC)

Capability tickets

- Matrix decomposition by row
- Appropriate for use in distributed environment
- Convenient and inconvenient aspects are opposite of ACL

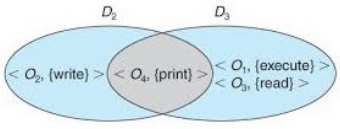


16

Discretionary Access Control (DAC)

Protection Domain

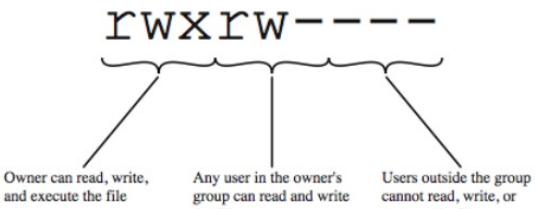
- Set of objects with associated rights
- In access matrix view, each row is a protection domain
  - But not necessarily just a user
  - May be a limited subset of user's access rights
  - Applied to a more restricted process
- May be static or dynamic



17

Discretionary Access Control (DAC)

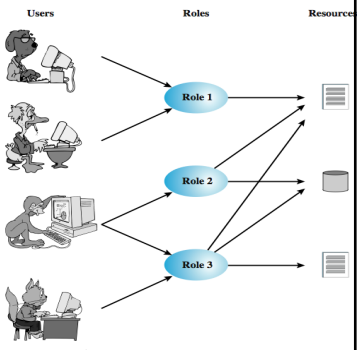
UNIX File Access Control



18

Role-Based Access Control (RBAC)

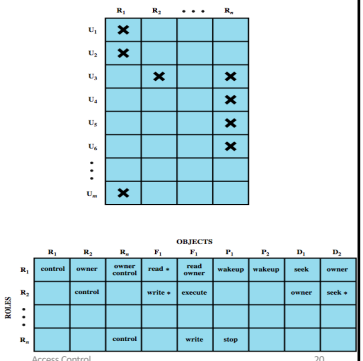
- Based on the roles that users assume in a system rather than the user's identity.
- Define a role as a job function within an organization.



19

Role-Based Access Control (RBAC)

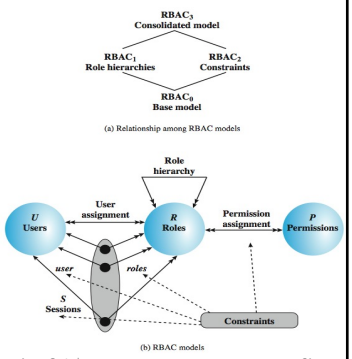
- Assign access rights to roles instead of individual users.
- Users are assigned to different roles, either statically or dynamically, according to their responsibilities.



20

Role-Based Access Control (RBAC)

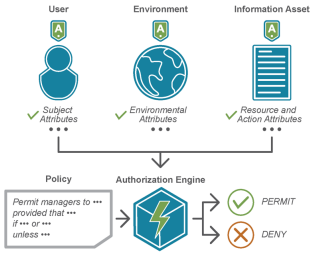
The many-to-many relationships between users and roles and between roles and permissions provide a flexibility and granularity of assignment not found in conventional DAC schemes.



21

Attribute-Based Access Control (ABAC)

ABAC can define authorizations that express conditions on properties of the resource and the subject.



The strength of ABAC is its flexibility and expressive power.

22

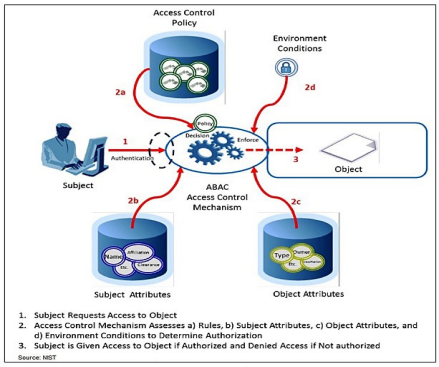
Attribute-Based Access Control (ABAC)

Key Elements of ABAC

- Attributes define specific aspects of subject, object, environment conditions, and requested operations. Types of attributes:
  - Subject attributes
  - Object attributes
  - Environment attributes
- Policy is set of rules and relationships that govern allowable behavior within an organization.
- Architecture applies to policies that enforce access control.

23

Attribute-Based Access Control (ABAC)



24

Other Access Control Models

- History Based Access Control (HBAC)

History of activities are used to determine access rights.

- Identity Based Access Control (IBAC)

Accesses are determined according to an individual.

- Organization Based Access Control (OrBAC)

Security policies are determined independently from implementations.

- Rule Based Access Control(RAC)

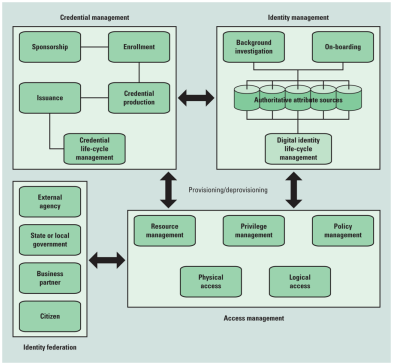
Preferred for specific contexts.

- ...

25

Identity, Credential, Access Management (ICAM)

ICAM is a comprehensive approach to managing and implementing digital identities, credentials, and access control.



26

Identity, Credential, Access Management (ICAM)

Identity Management

- Assigns attributes to a digital identity and connects that digital identity to an individual.
- The goal is to establish a trustworthy digital identity that is independent of a specific application or context.

Credential Management

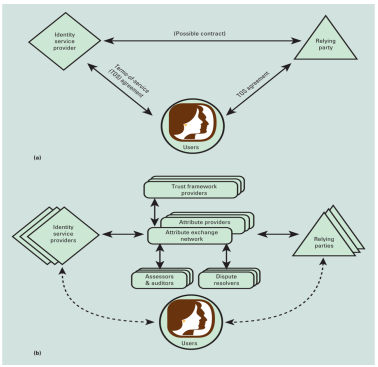
- Is the management of the lifecycle of credentials.

Access Management

- Deals with the management and control of the ways entities are granted access to resources

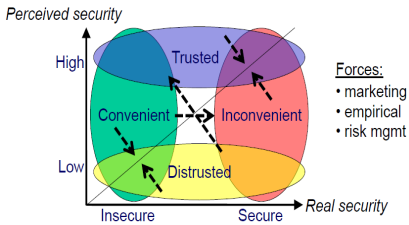
27

Trust Frameworks



28

Trust and Security



Forces:
- marketing
- empirical
- risk mgmt

*Josang

Problem

Can I trust to the security system of a specific service based on my private needs?

29

Definition of Trust

Gambetta for Social Sciences

The subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends.

Grandison and Sloman for Computer Networks and Security

The firm belief in the competence of an entity to act dependable, securely and reliably within a specified context.

Massa for Online Social Networks

The judgment expressed by one user about another user, often directly and explicitly, sometimes indirectly through an evaluation of the artifacts produced by that user or her activity on the system.

30

Origin of Trust

≠

Real (Assumed) Fact

- **Characteristics:** crisp, frequenist
- **Formalisms:**
  - binary logic
  - quantum logic

Perceived Fact

- **Characteristics:** vague, fuzzy, uncertain
- **Formalisms:**
  - subjective probabilities
  - multi-valued logic
  - probabilistic logic

31

Where Does Trust Reside?

Trust Relationship

assess

marketing

Trustor (trusting party)

- is a situation of dependence
- wants to assess and make decision about trustee (Josang)

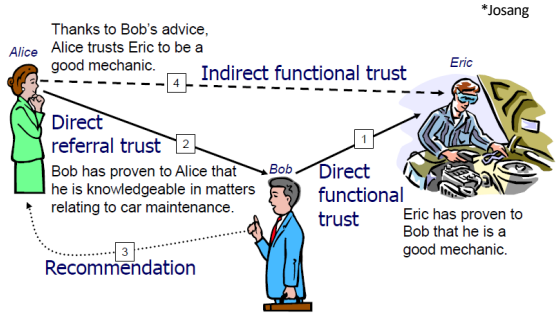
Trustee (trusted party)

- is a situation of power and expectation to deliver
- wants to represent and put in a positive light own competence (Josang)

32

General Trust Models

*Josang



33

Summary

- Access control functions
- Principles, policies, requirements
- Elements: subject, object, access rights
- DAC, MAC, RBAC, ABAC, Management and Trust frameworks

34