UMBC

Dr. Roberto Yus

https://robertoyus.com/

Data Privacy

CMSC 463/663

L05 – Access Control

Icons from https://thenounproject.com/

Previously on…

- Usable Privacy → HCI is critical for privacy
- Informed Consent
  - P3P
  - Automated Analysis of Privacy Policies

GOOGLE / TECH / PRIVACY

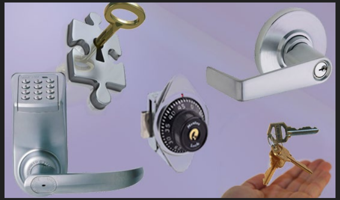
Mozilla study lambasts Google over ‘misleading’ privacy labels on top Android apps

In the news!

Access Control

“selective **restriction of access** to a place or other resource”

Physical Security



Computer Security

Components

- **Access control policy**
  - Specifies the authorized accesses of a system
- **Access control mechanism**
  - Implements and enforces the policy

Entities

- **Subjects**
  - Entity that can access objects
- **Objects**
  - Access controlled resource
    - Files, records, directories, etc.
- **Access right**
  - Way in which subject accesses object
    - Read, write, execute, delete, create, search, etc.

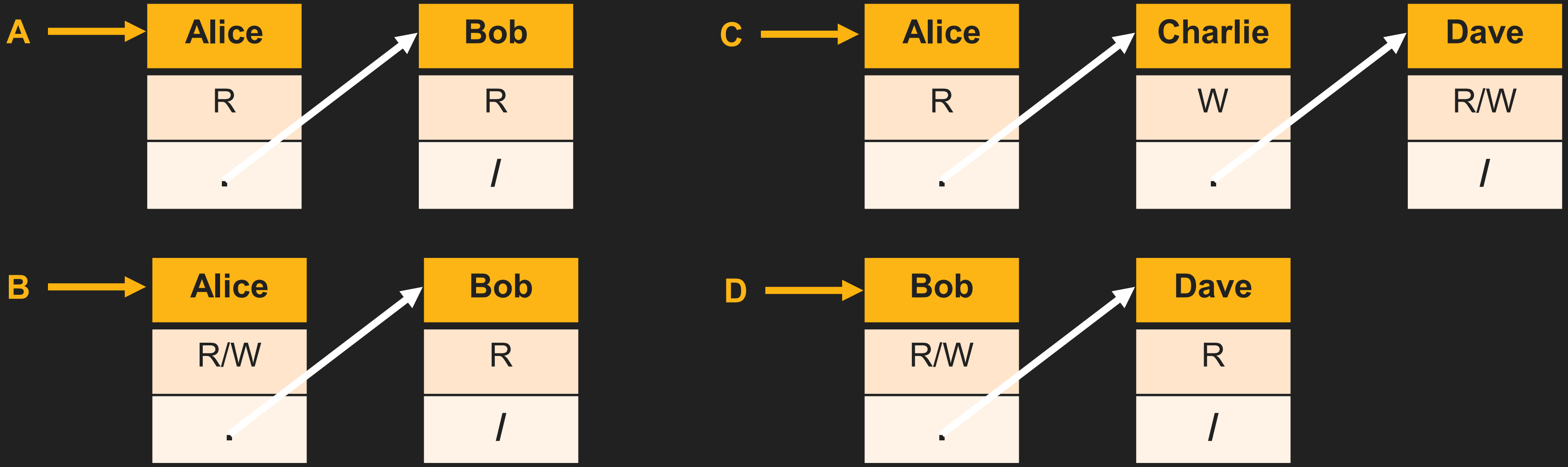
Access Control Matrix

		Objects			
		A	**B**	**C**	**D**
Subjects	**Alice**	*R*	*R/W*	*R*	-
	Bob	*R*	*R*	-	*R/W*
	Charlie	-	-	*W*	-
	Dave	-	-	*R/W*	*R*

Grouping

		System Files		User Files	
		A	B	C	D
Staff	Alice	*R*	*R/W*	*R*	-
	Bob	*R*	*R*	-	*R/W*
Students	Charlie	-	-	*W*	-
	Dave	-	-	*R/W*	*R*

Access-Control List (ACL)



- Convenient wrt objects
- Difficult to determine all objects a subject can access

Real world example?

JULIA EVANS
@b0rk

unix permissions

drawings.jvns.ca

There are 3 things you can do to a file

read write execute

ls -l file.txt shows you permissions
Here's how to interpret the output:

```
rw-   rw-   r--   bork staff
```

bork (user) can read & write

staff (group) can read & write

ANYONE can read

File permissions are 12 bits

```
setuid setgid
000     110    110    100
sticky  user   group  all
        rwx    rwx    rwx
```

For the r/w/x bits:

1 means "allowed"

0 means "not allowed"

110 in binary is 6

```
So  rw-   r--   r--
  = 110   100   100
  = 6     4     4
```

chmod 644 file.txt means change the permissions to:

rw- r-- r--

simple!

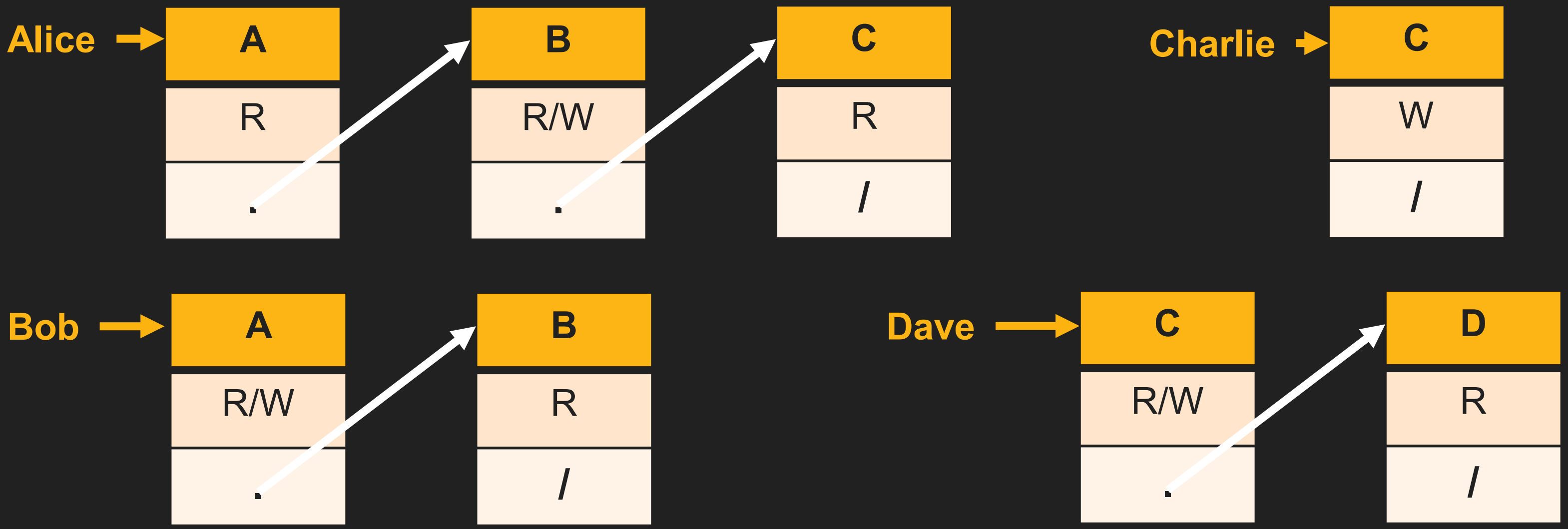
setuid affects executables

```
$ ls -l /bin/ping
rws r-x r-x root root
```

this means ping always runs as root

setgid does 3 different unrelated things for executables, directories, and regular files

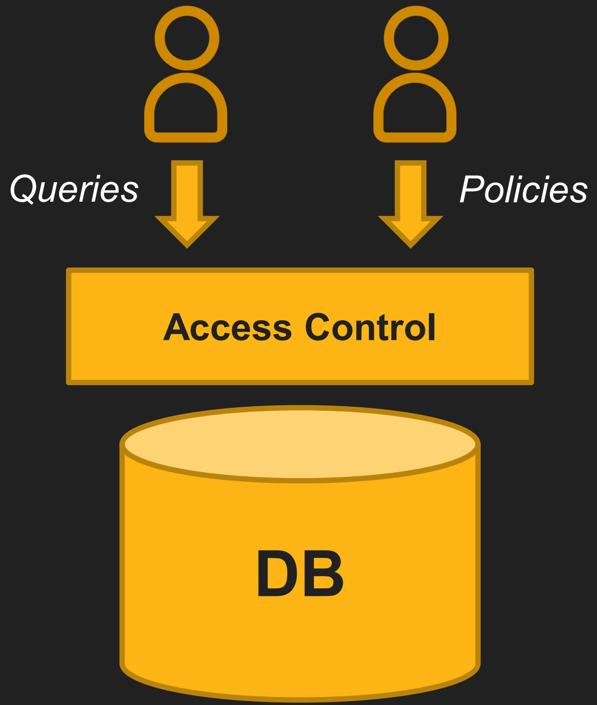
Capability-Based



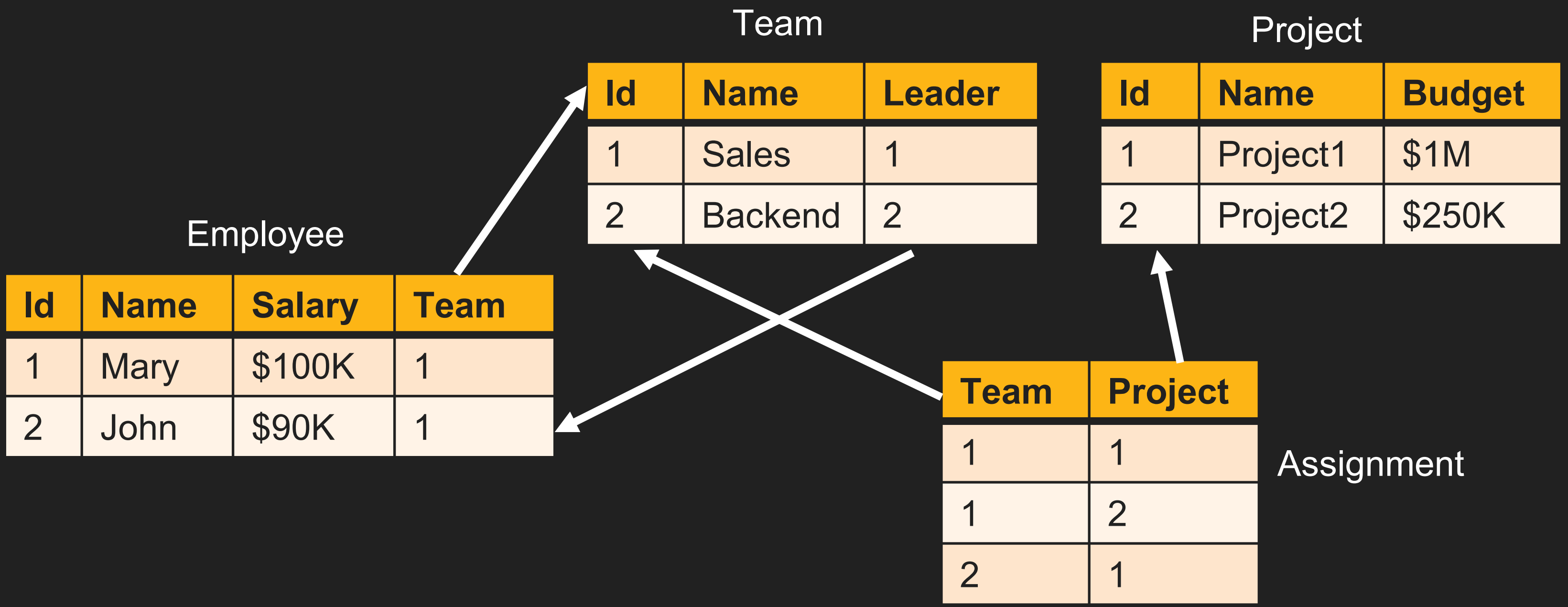
- Convenient wrt subjects
- Difficult to determine all subjects that can access object

Access Control Policy Models

- **Attribute-based Access Control (ABAC)**
- **Discretionary Access Control (DAC)**
- Graph-based Access Control (GBAC)
- History-Based Access Control (HBAC)
- History-of-Presence Based Access Control (HPBAC)
- Identity-Based Access Control (IBAC)
- Lattice-Based Access Control (LBAC)
- **Mandatory Access Control (MAC)**
- Organization-Based Access control (OrBAC)
- **Role-Based Access Control (RBAC)**
- Rule-Based Access Control (RAC)
- Responsibility Based Access control
- …



Databases 101



Team

Id	Name	Leader
1	Sales	1
2	Backend	2

Project

Id	Name	Budget
1	Project1	$1M
2	Project2	$250K

Employee

Id	Name	Salary	Team
1	Mary	$100K	1
2	John	$90K	1

Assignment

Team	Project
1	1
1	2
2	1

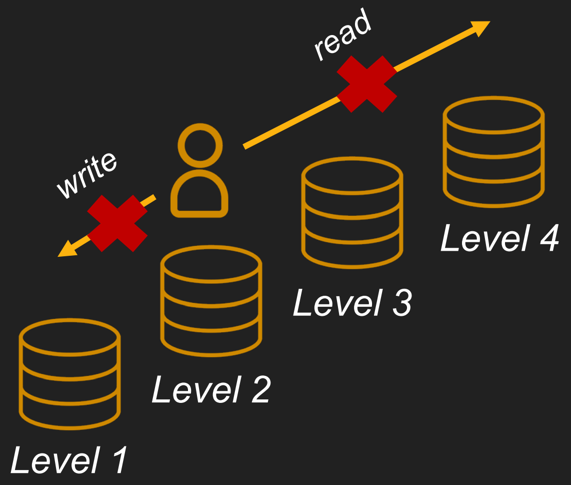
```
SELECT E.Name, E.Salary
FROM Employee E, Project P, Assignments A
WHERE P.Name=“Project1” AND P.Id=A.Project AND E.Team=A.T
```

Mandatory Access Control (MAC)

- Provide users with access **based on data confidentiality and user clearance levels**
- Access is granted on a **need-to-know** basis
- Policies **defined by administrators** not by users
- Based on **multilevel security** (MLS)
  - Top secret > secret > confidential > restricted > unclassified

MAC: Properties

- Two required properties for confidentiality:
  - **No read up**
    - Subject can only read an object of less or equal security level
  - **No write down**
    - Subject can only write into object of greater or equal security level



MAC: Mechanism

Project

Id	Name	Budget
1	Project1	$1M
2	Project2	$250K

Project-MAC

Id	*λ(Id)*	Name	*λ(Name)*	Budget	*λ(Budget)*

Top-Secret User

Id	*λ(Id)*	Name	*λ(Name)*	Budget	*λ(Budget)*
1	*S*	Project1	*S*	$1M	*TS*
2	*S*	Project2	*S*	$250K	*TS*

Secret User

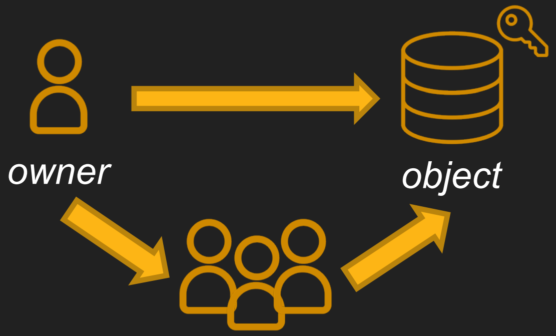
Id	*λ(Id)*	Name	*λ(Name)*	Budget	*λ(Budget)*
1	*S*	Project1	*S*	null	*S*
2	*S*	Project2	*S*	null	*S*

MAC: Pros and Cons

- **Pros**
  - Increased security & confidentiality/privacy protection
- **Cons**
  - Difficult to implement granularity
  - Difficult to maintain

Discretionary Access Control (DAC)

- For **each subject** access right to the objects are defined
  - (subject, object, +/- access mode)
  - (Mary, Project, read)
- **Owner decides access**
- Mechanisms:
  - Grant & Revoke
  - Views
  - Query Modification



Specifies users who can access

DAC: Grant and Revoke

GRANT *<privilege>* ***ON*** *<relation>* ***TO*** *<user>*

- GRANT SELECT * ON Project TO Mary
- GRANT SELECT(Salary) ON Employee TO John

REVOKE *<privileges> [***ON*** <relation>]* ***FROM*** *<user>*

- REVOKE SELECT * ON Project FROM John
- REVOKE SELECT(Salary) ON Employee FROM Mary

DAC: Views

```
CREATE VIEW Small-Projects
AS SELECT Id, Name, Budget
    FROM Project
    WHERE Budget < $500K
```

Assign rights to access a limited part of the data

DAC: Query Modification

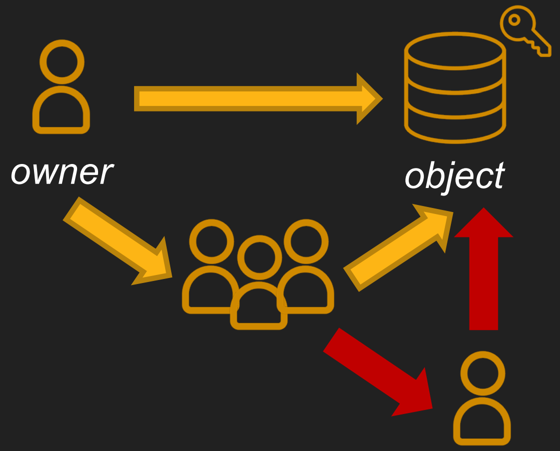
- Limit the queries a user can pose by rewriting them

- John → ***SELECT*** * ***FROM*** *Projects*

- Modified query → ***SELECT*** * ***FROM*** *Projects* ***WHERE Budget < $500K***

DAC: Pros and cons

- **Pros**
  - User-friendly
  - Flexible
  - Easy to implement
  - Granular (up to some extent…)
- **Cons**
  - Lower level of data protection
  - Difficult to maintain

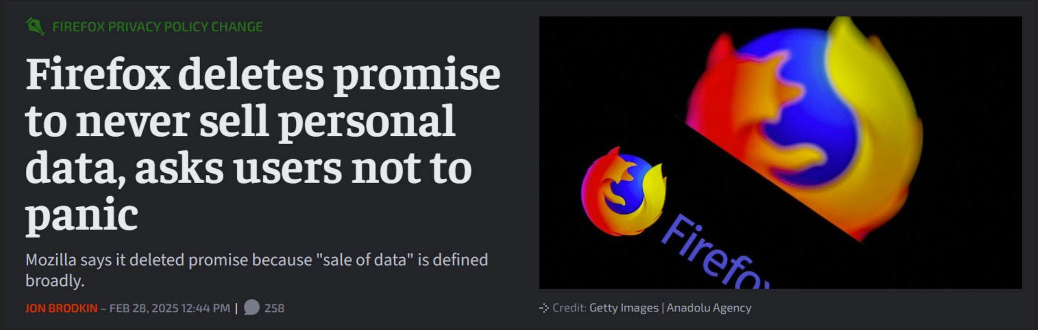


Group Activity

- Choose a service (e.g., your project or a Web service / App)
- Think of examples of
    - Mandatory Access Control (MAC) policies
    - Discretionary Access Control (DAC) policies
- Is there anything you want to define that is not possible with MAC or DAC?

Previously on…

- Access Control
  - Physical vs Computer Security
- Mandatory Access Control (MAC) vs. Discretionary Access Control (DAC)



FIREFOX PRIVACY POLICY CHANGE

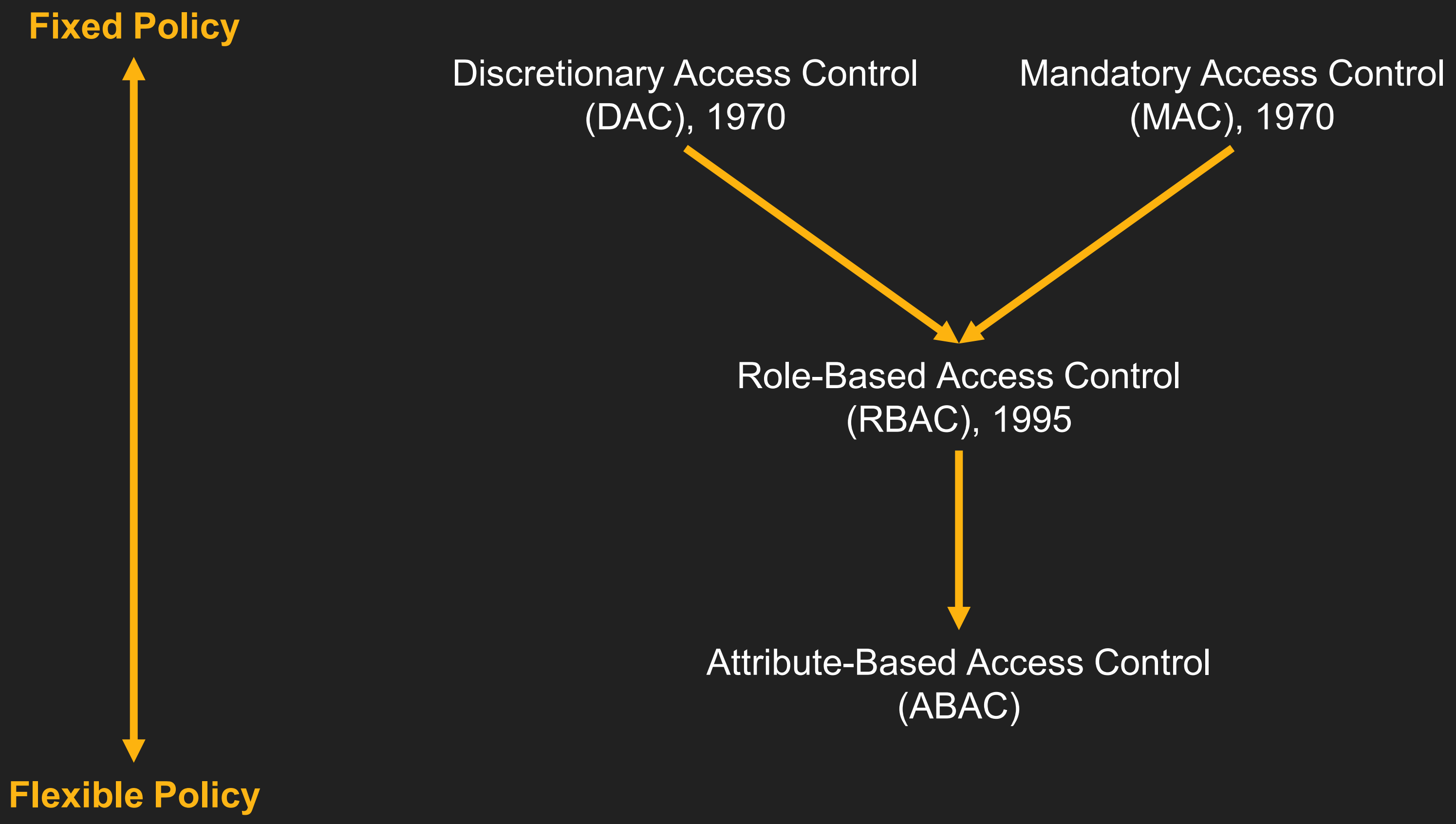
Firefox deletes promise to never sell personal data, asks users not to panic

Mozilla says it deleted promise because "sale of data" is defined broadly.

JON BRODKIN – FEB 28, 2025 12:44 PM | 258

Credit: Getty Images | Anadolu Agency

In the news!



Fixed Policy

Flexible Policy

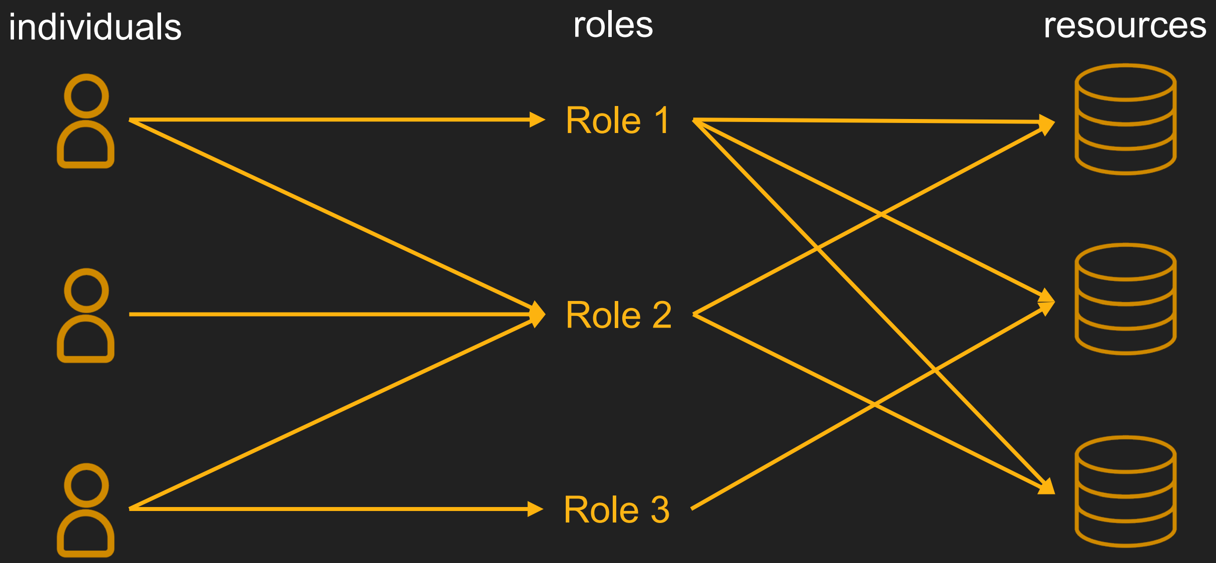
Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role-Based Access Control (RBAC), 1995

Attribute-Based Access Control (ABAC)

Role-Based Access Control (RBAC)



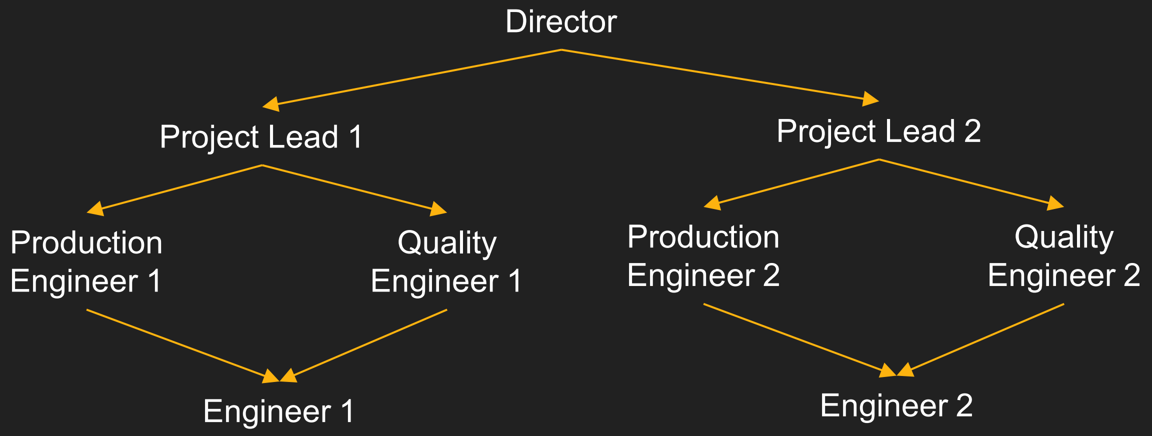
- **Access determined by roles**
  - Individuals change frequently but roles not that much!

RBAC: How does it work?

- Administrator defines roles
  - *E.g., RA, TA, grader, instructor, professor, etc.*
- Security administrator define RBAC policies for different roles
  - *E.g., (grader, homework, read), (TA, grade, read), (instructor, grade, write), …*
- Administrator assign roles to individuals
  - *E.g., Roberto → instructor, professor ; Mary → TA ; John → grader*

RBAC: is it MAC / DAC / Neither?

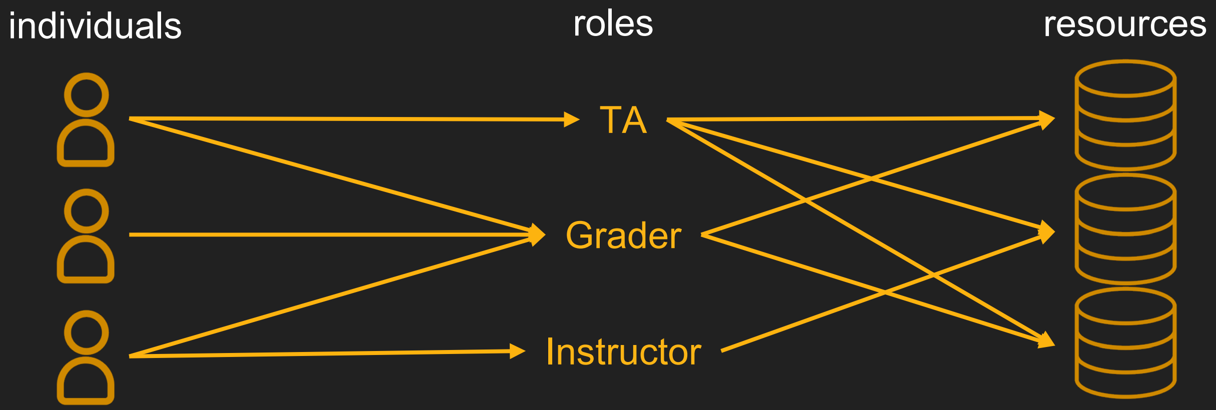
- **RBAC is policy neutral**
  - Both MAC and DAC can be implemented with RBAC



Hierarchy of roles:

Upper roles have access rights of lower roles

RBAC: Challenges



- What if I want to define different access for my TA?
  - New role: TA_DataPrivacy!
  - Role explosion! TA_DataPrivacy, TA_CMSC331, TA_CMSC331_Fall….?
- What if I want to define access based on context?
  - New role: TA_DataPrivacy_Grading !?

Attribute-Based Access Control (ABAC)

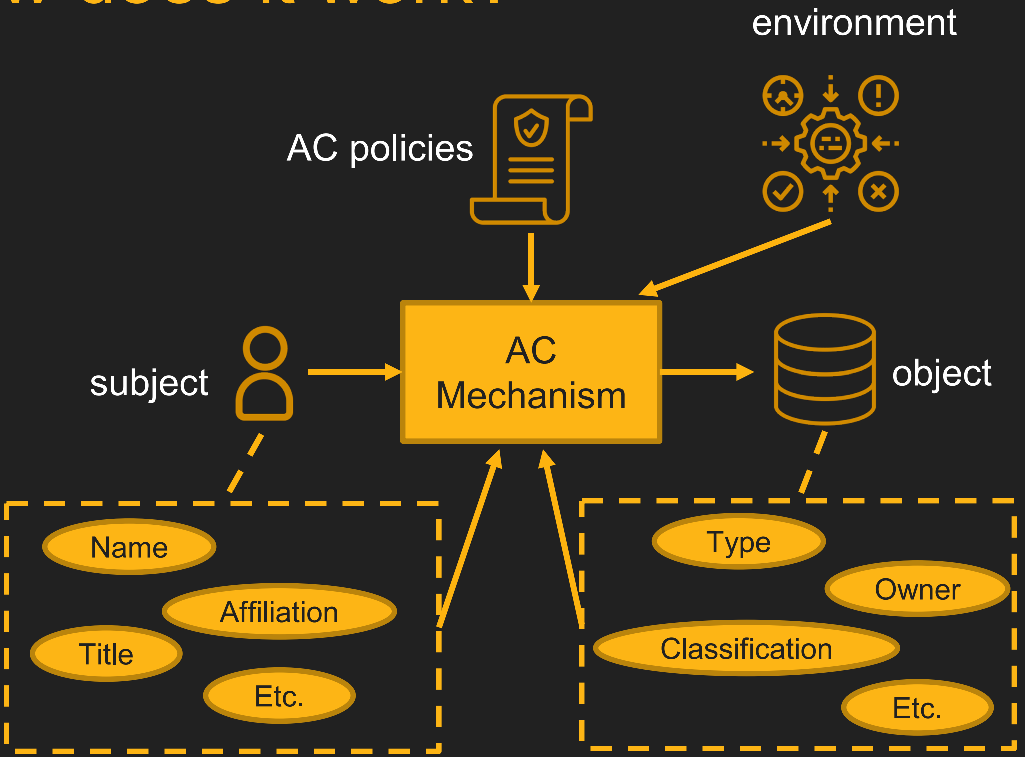
- Define authorizations that express **conditions on properties of both the resource and the subject**
  - Each resource has an attribute (e.g., the subject that created it)
  - A single rule states ownership privileges for the creators
- Increased **flexibility** and **expressivity** power

ABAC: Attributes

- **Subject**
  - Define identity and characteristics
  - E.g., name, organization, job title, etc.
- **Object**
  - Define the characteristics of the resource
  - E.g., title, author, date
- **Environment attributes**
  - Describe the operational, technical, and even situational environment or context in which the information access occurs
  - E.g., current date, network security level
  - **Not associated with a resource or subject**

ABAC: How does it work?

1. Subject requests access to Object
2. AC governed by policies: assesses the attr of subject, object, and env
3. AC grants subject access to object if authorized



Other Access Control Policy Models

Graph-based Access Control (GBAC)

History-Based Access Control (HBAC)

History-of-Presence Based Access Control (HPBAC)

Identity-Based Access Control (IBAC)

Lattice-Based Access Control (LBAC)

Organization-Based Access control (OrBAC)

Rule-Based Access Control (RAC)

Responsibility Based Access control

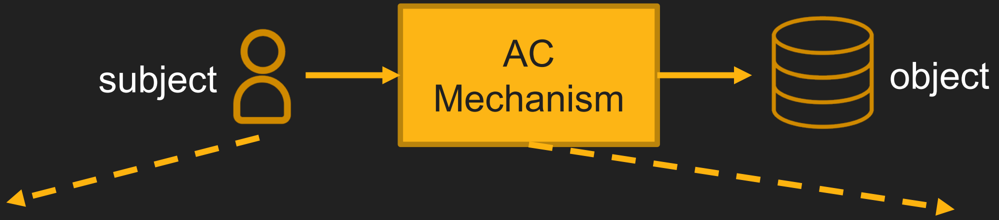
…

AC: Open Challenges

- In addition to new models, **new AC mechanisms are required**
- **AC implementation** in new domains (IoT, Big Data, AI, Cloud computing, etc.) brings **new challenges**
  - Inference problem
  - Semantic gap
  - Scalability!
  - …

AC: Open Challenge

- The **inference problem**
  - Can the subject gain access to the object even if we don’t grant it?
  - Use other information to infer the protected object



Name	Grade
John	A
Mary	A
Dave	F

SELECT grade **FROM** Student

SELECT grade **FROM** Student ***WHERE grade > D***

Name	Grade
John	A
Mary	A

I know that Dave is enrolled in the class

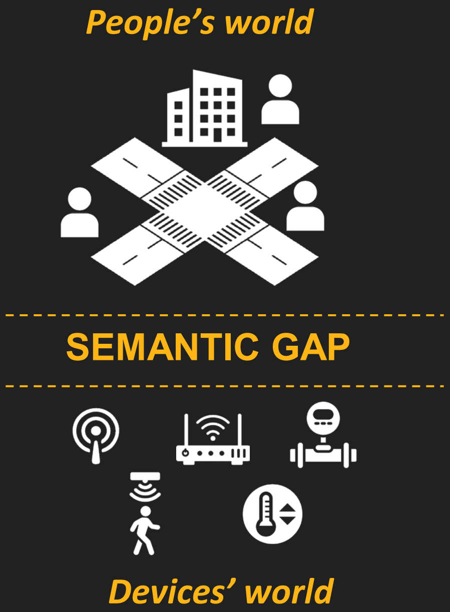
Dave got an F or D!

AC: Open Challenge

- The **Semantic Gap problem**

*“Do not **track** my **location**”*

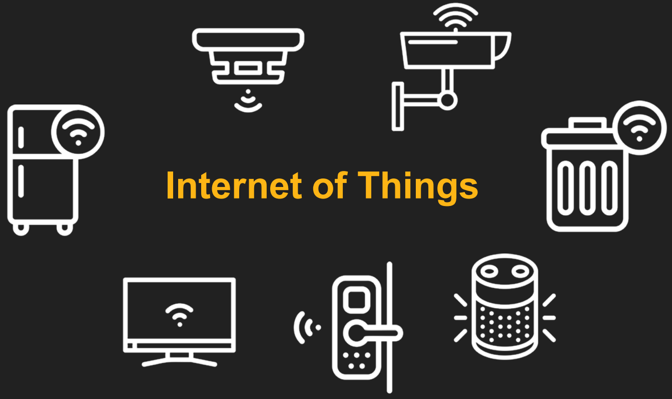
*“Do not **share** my **social interactions** with applications”*



People’s world

SEMANTIC GAP

Devices’ world



Internet of Things

```
2016-01-15 17:38:07.463623 | DISMAN-EVENT-
MIB::sysUpTimeInstance = Timeticks:
(167664600) 19 days, 9:44:06.00 SNMPv2-
MIB::snmpTrapOID.0 = OID: SNMPv2-
SMI::enterprises.14179.2.6.3.53 SNMPv2-
SMI::enterprises.14179.2.6.2.35.0 = Hex-
STRING: 00 19 A9 55 CE B0 NMPv2-
SMI::enterprises.14179.2.6.2.36.0 = INTEGER:
1 SNMPv2-SMI::enterprises.14179.2.6.2.43.0 =
IpAddress: 169.234.57.122
```

What should I protect?

Summary

- Access Control restricts access to resources
- Useful to represent user privacy preferences
- Two parts:
    - AC Policy + AC Mechanism
- Plenty of AC models!
    - DAC / MAC, RBAC, ABAC, …
- Open challenges for AC mechanisms

Group Activity

- Choose a service (e.g., your project or a Web service / App)
- Think of examples of Attribute-Based Access Control (ABAC) policies:
    - Defined by the administrator for employees
    - Defined by users of the service