Decomposing ABAC into Explicit combination of DAC and Attribute Constraints

Guide : Prof. R.K. Shyamasundar

Sejal Patel- 163050093

Access Control Model

It decides whether subjects is allowed to access the objects or not.
It protects privacy and integrity of the data.
Unauthorized access might cause

- data loss
- data misuse
- information leak
- modify data

Access Control Model

To ensures safety, privacy and integrity of the data/information access control are used.

Exampes

- Username password
- Token
- Biometric

Traditional Aceess Control Models

- Discretionary Access Control Model
- Mandatory Access Control Model
- Role-Based Access Control Model
- Attribute Based Access Control Model

Discretionary Access Control

- Restriction on access of the objects based on identity of requester.
- Owner determines “which subject will access what objects”.
- Access can be passed on from one to another.
- It does not have any control over information flow.

Example of DAC

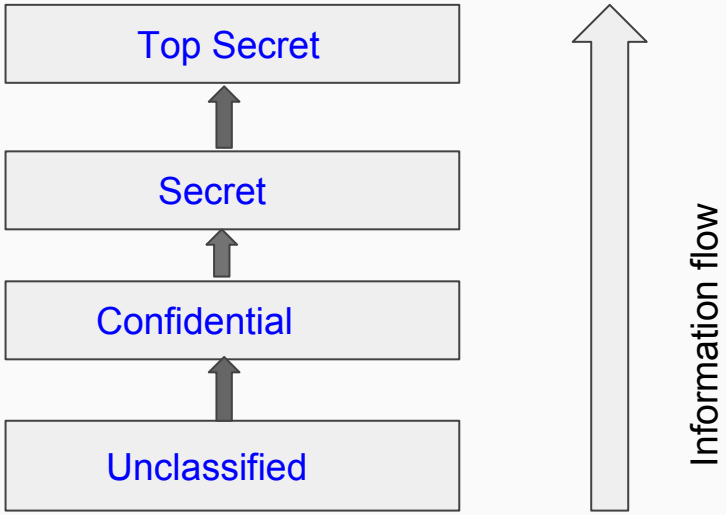
Representation of DAC Policy

	Object 1	Object 2	Object 3
User 1	read,write	write	
User 2		read	
User 3	write		read,write

Mandatory Access Control

Multiple security level in terms of hierarchy .

Subject : Clearance
Object : Clasification



MAC Continued..

- Subject with clearance x can access all object in x and below x.
- Information only flow upward.
- Generally used for confidential and classified information.
- Used in Military and government software.

Role Based Access Control

Role : collection of permission based on requirements

- Access is granted to user via role
- Users are assigned a specific role
- Users can be assigned multiple role

Representation of RBAC

User to Role Mapping

Users	**Role**
User1, User2	Doctor
User3	Nurse

Role to Permission Mapping

Role	**Permissions**
Doctor	Prescribe medicine, view medical record of patients
Nurse	View basic data, give medicine to patients

- Prefered for large user population
- Different requirement leads to new role
- Does not consider parameters like time, day, and location of access object metadata, environment context

Attribute Based Access Control

- Access rights are based on attributes of subject and object.
- Some attributes are dynamic, for example time of day.
- Attributes are classified into three type

  Subject's Attribute : id, name, role

  Object's Attribute : file_type, owner, last modified date

  Environment attribute : time, day, location

ABAC is prefered

- For time based policies :- deny access outside office hours
- Location based policies :- cashier allowed to change daily transaction report in bank only.
- Time constraints :-employees who completed 12 hrs of training on a particular platform should be allowed.

Decision Table

- A way to represent an ABAC rule .
- Represents relationships between attributes of the subject and object.
- Each column defines an access control decision provided attribute values.
- It makes it easy to see all the different combination that has to be considered.

	R1	R2	R3	R4
Student	T		T	
Faculty		T		T
Book	T			T
Account		T	T	
Borrow	T			
Read		T	T	
Return				T
Holiday		T		T
Working	T		T	
Permission	P	P	P	P

Sample Decision Table

Sample Decision Table

Decomposition of Decision Table

Student is allowed to borrow book **If** :

(day == “working”) ∧ clearance(student) == “secret”
∧ security level(book) == “unclassified”
∧ time(activity)= “within working hours”.

- check if student is allowed to borrow book
- if it is allowed check for attribute constraints.

DAC Table

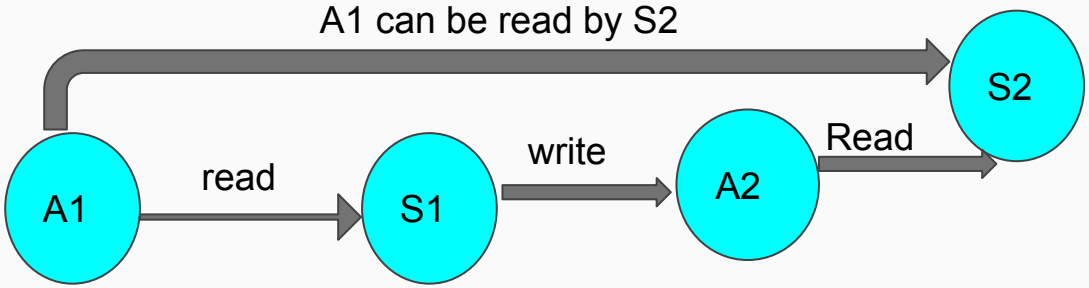
	book	account
student	borrow1,	
faculty		read2

Attribute Table

Entry No.	Day
1	Working
2	Holiday

Indirect Flow

S1 can read an object A1.
S1 can write an object A2.
S3 can read an object A2.



Detection of Indirect Flow

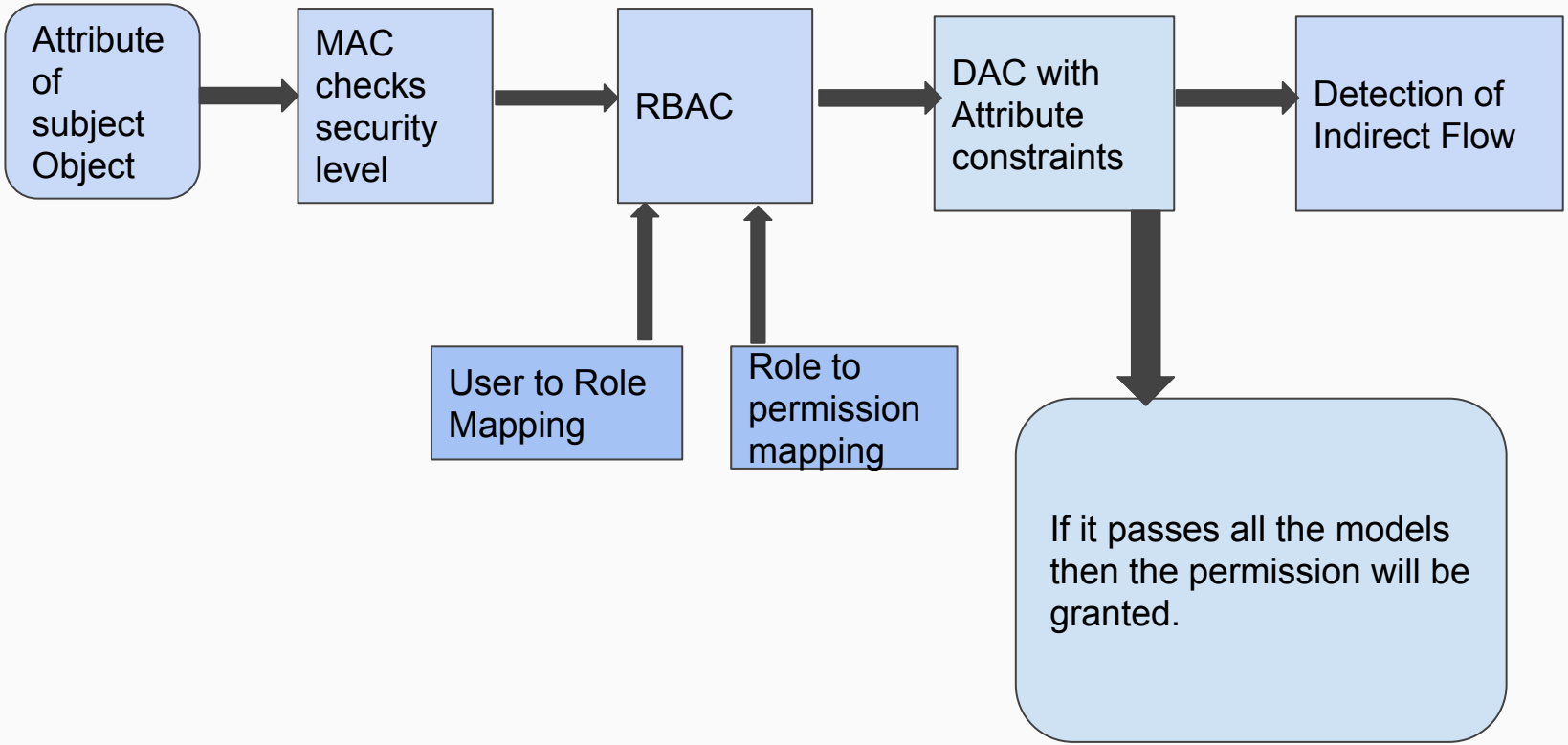
Matrix representation

	A1	A2	S1	S2
S1		1		
S2				
A1			1	
A2				1

Transitive closure

	1		
		1	1
			1

Our Method


Attribute of subject Object
MAC checks security level
RBAC
DAC with Attribute constraints
Detection of Indirect Flow
User to Role Mapping
Role to permission mapping
If it passes all the models then the permission will be granted.

Comparison Table

Category	Decision table in ACPT	Our approach
Attribute types	Basic data types	Basic data types
Attribute domains	Explicit specification	Explicit specification
Attribute classification	Subjects, resources, Actions, environments	Subject, resources, action
Access decision	Permit ,Deny	Permit ,Deny
Default access decisions	Yes	Yes
Formalism of rules	Decision table / Propositional logic	Decision table
User-defined functions	No	NO
Conflict resolution	Explicit operators	Explicit operators
Query	Combination of all attributes	Combination of all attributes

THANK YOU !