

Access Control Evolution and Prospects

Ravi Sandhu
Executive Director

Professor of Computer Science
Lutcher Brown Chair in Cyber Security

October 2019

ravi.sandhu@utsa.edu
www.ics.utsa.edu
www.profsandhu.com

Objectives

POLICY

ATTACKS

Enable
↕
Enforce

What?

Why?

Respond
↕
Defend

Mechanisms

P
R
O
T
E
C
T

How?



Complement

D
E
T
E
C
T

- Access Control: Authentication, Authorization
- Cryptography: Symmetric, Assymmetric
- Detection: Signature, Zero Day
- Recovery/Recourse: Backups, Forensics
- Tolerance/Resilience: Mission Assurance
-

- Copy control
- Inference
- Analog hole
- Trusting humans vs trusting software
- Trusted computing base vulnerabilities
- Side channels and covert channels
-

Symmetric Key Cryptography, 1977

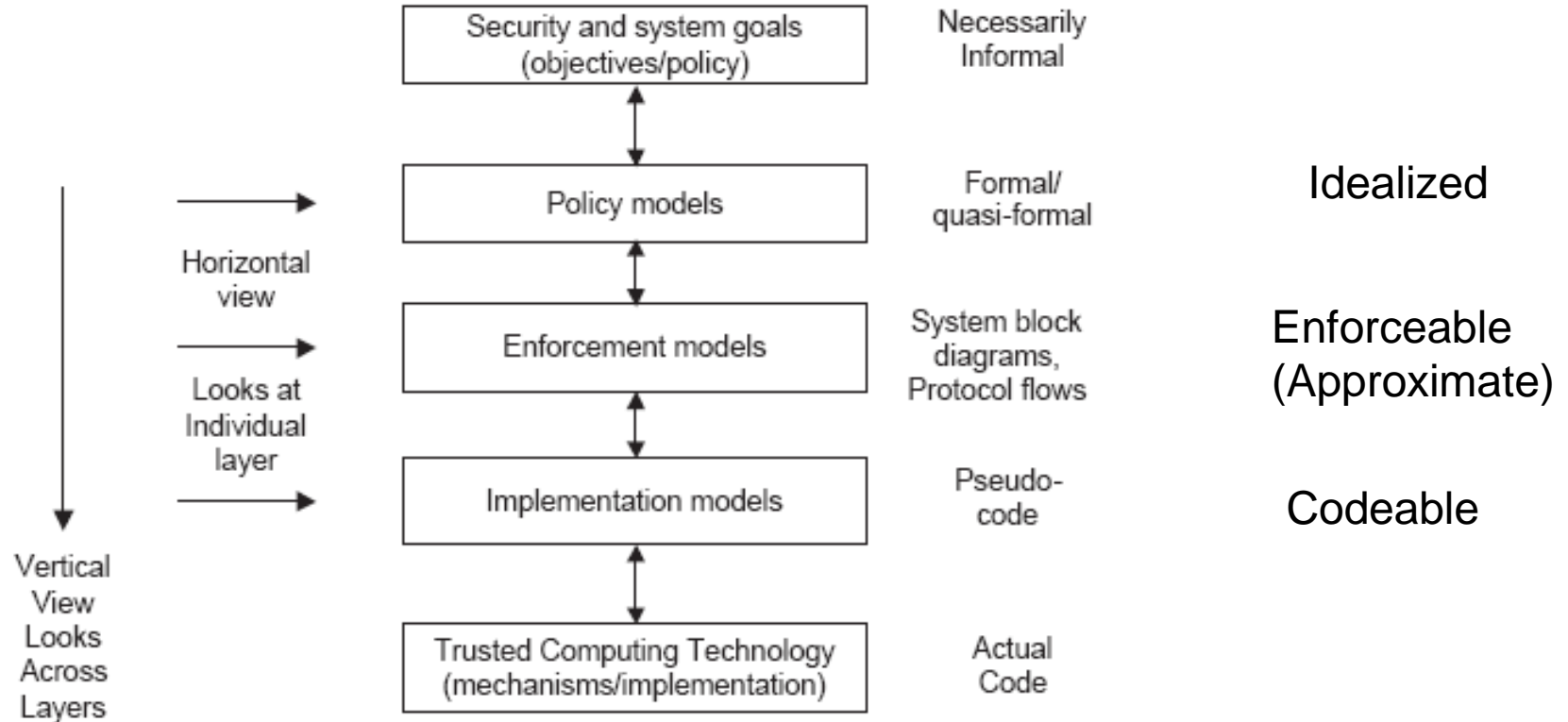


Asymmetric Key Cryptography, 1996



BlockChain Applications, ????

Assumes Successful Authentication



**Discretionary Access Control
(DAC), 1970**

**Mandatory Access Control (MAC),
1970**

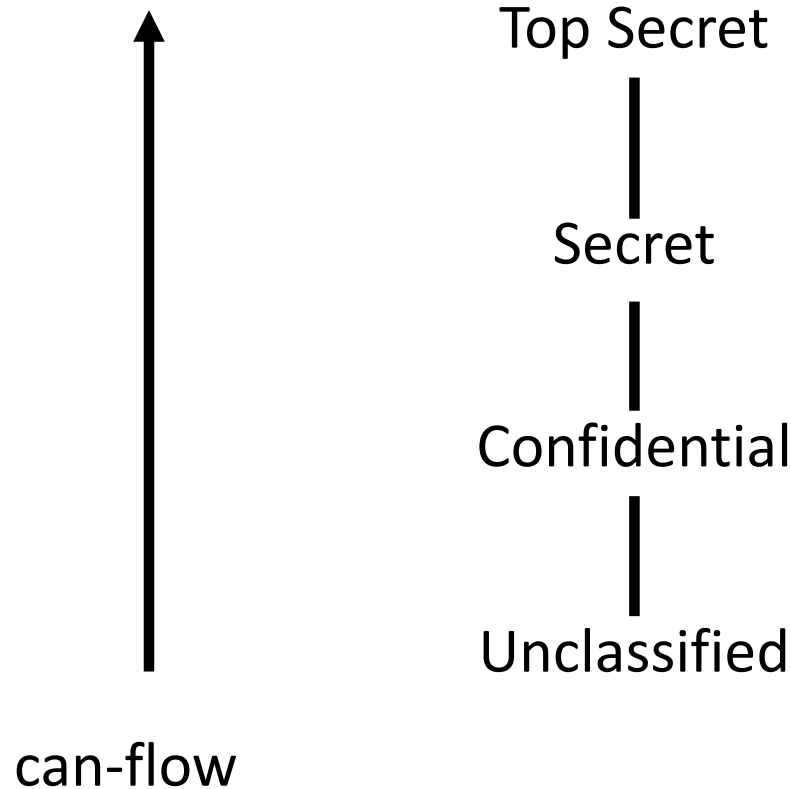


**Role Based Access Control
(RBAC), 1995**



**Attribute Based Access Control
(ABAC), ????**

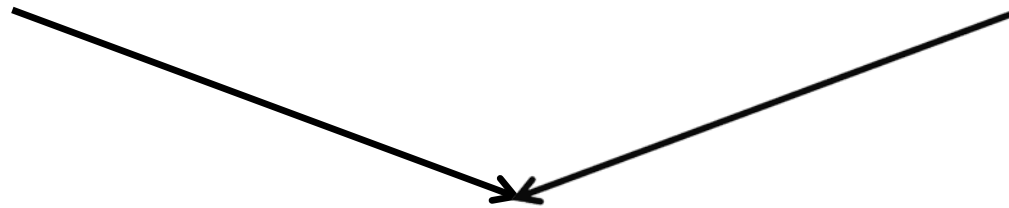
- Core concept:
 - Custodian of information determines access
- Core drawback:
 - Does not protect copies
 - Therefore OK for integrity but not for confidentiality
- Sophistication:
 - Delegation of custody
 - Denials or negative rights



- Core concept:
 - Extend control to copies by means of security labels
- Core drawback:
 - Covert/side channels bypass MAC
 - Inference not prevented
 - Too strict
 - Too reductionist
- Sophistication:
 - Dynamic labels

**Discretionary Access Control
(DAC), 1970**

**Mandatory Access Control (MAC),
1970**



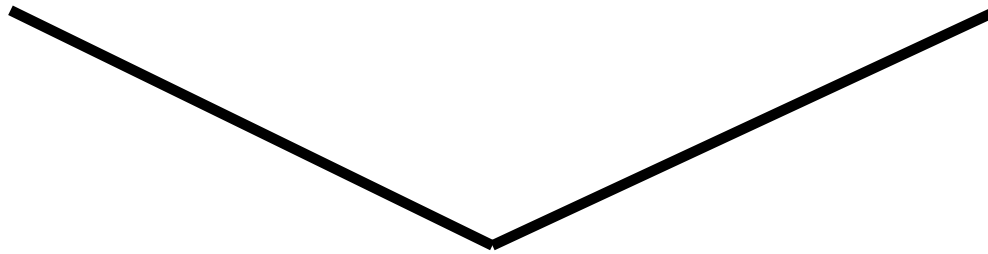
**Role Based Access Control
(RBAC), 1995**



**Attribute Based Access Control
(ABAC), ????**

**Primary-Care
Physician**

**Specialist
Physician**



Physician



Health-Care Provider

- Core concept:
 - Roles determine everything
- Core drawback:
 - Roles are a natural concept for human users
 - But not so natural for:
 - Information objects
 - IoT things
 - Contextual attributes
- Sophistication:
 - Role hierarchies
 - Role constraints

- Fundamental theorem of RBAC:
 - RBAC can be configured to do DAC
 - RBAC can be configured to do MAC

**Discretionary Access Control
(DAC), 1970**

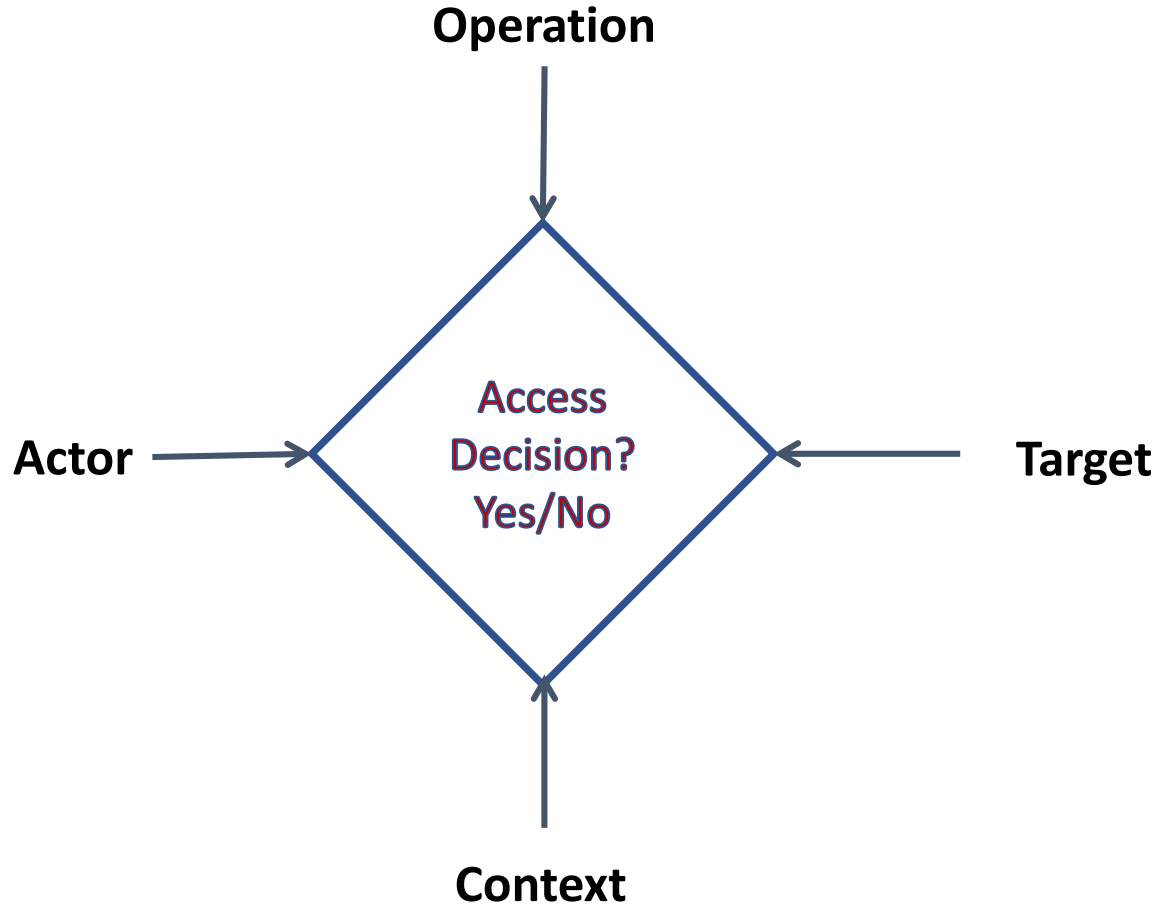
**Mandatory Access Control (MAC),
1970**



**Role Based Access Control
(RBAC), 1995**



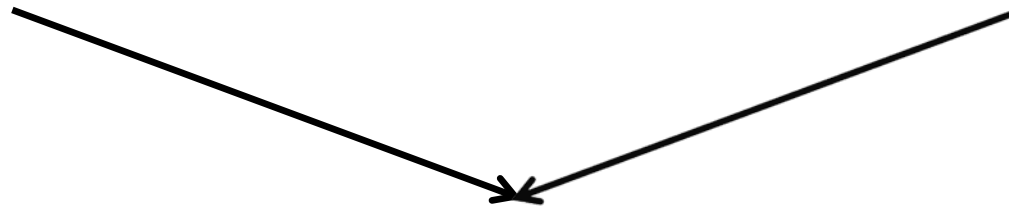
**Attribute Based Access Control
(ABAC), ????**



- Core concept:
 - Attributes determine everything
 - No fixed access decision rule
- Core drawback:
 - Flexibility at the cost of complexity
- Sophistication:
 - Chained attributes
 - Group attributes
 - Distributed decision rules
 - Automation
 - Adaptation

**Discretionary Access Control
(DAC), 1970**

**Mandatory Access Control (MAC),
1970**



**Role Based Access Control
(RBAC), 1995**



**Attribute Based Access Control
(ABAC), ????**

7. ABAC Design, Engineering and Applications

5. ABAC Policy
Architectures
and Languages

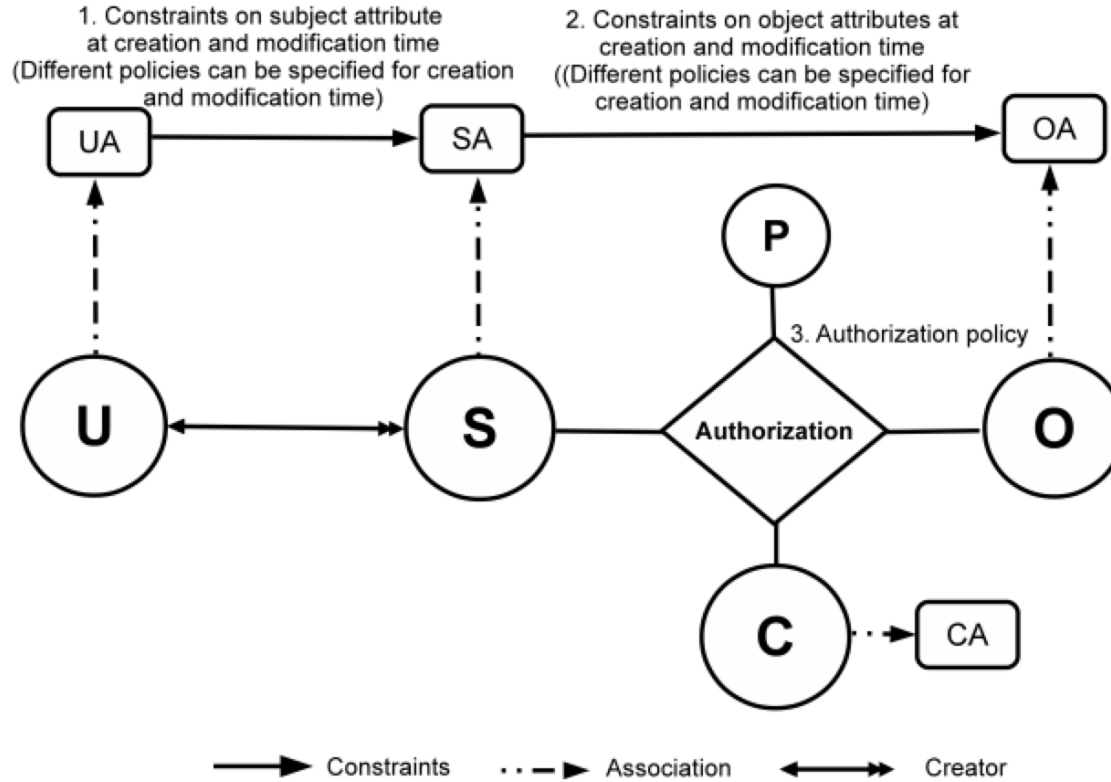
3. Administrative
ABAC Models

4. Extended
ABAC Models

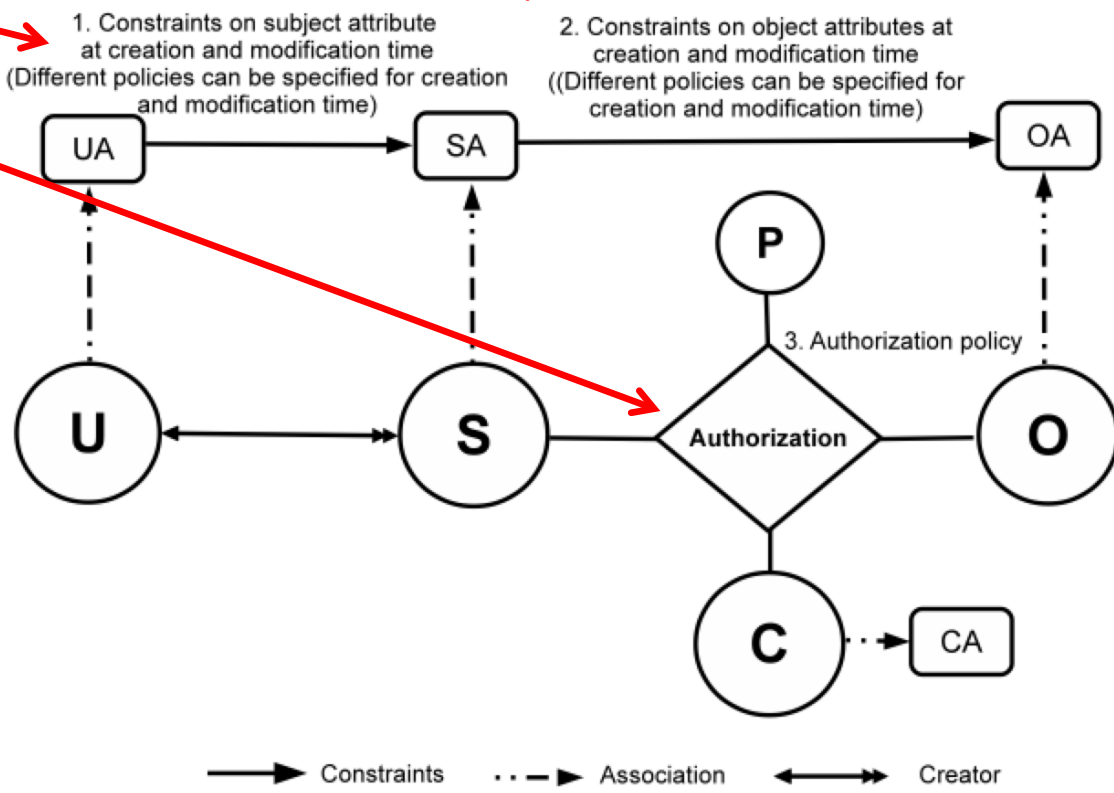
6. ABAC
Enforcement
Architectures

2. Core ABAC Models

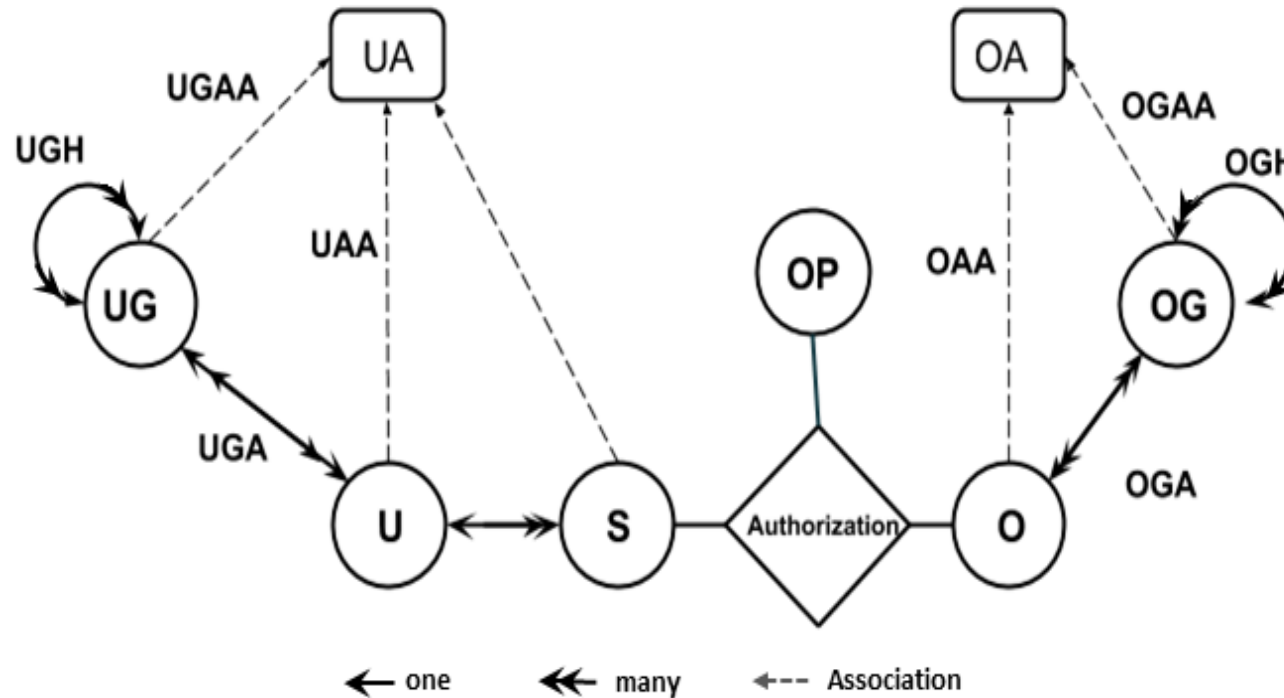
1. Foundational Principles and Theory



**Policy
Configuration
Points**



Can be configured to do various forms of DAC, MAC, RBAC (Jin, Krishnan, Sandhu 2012)

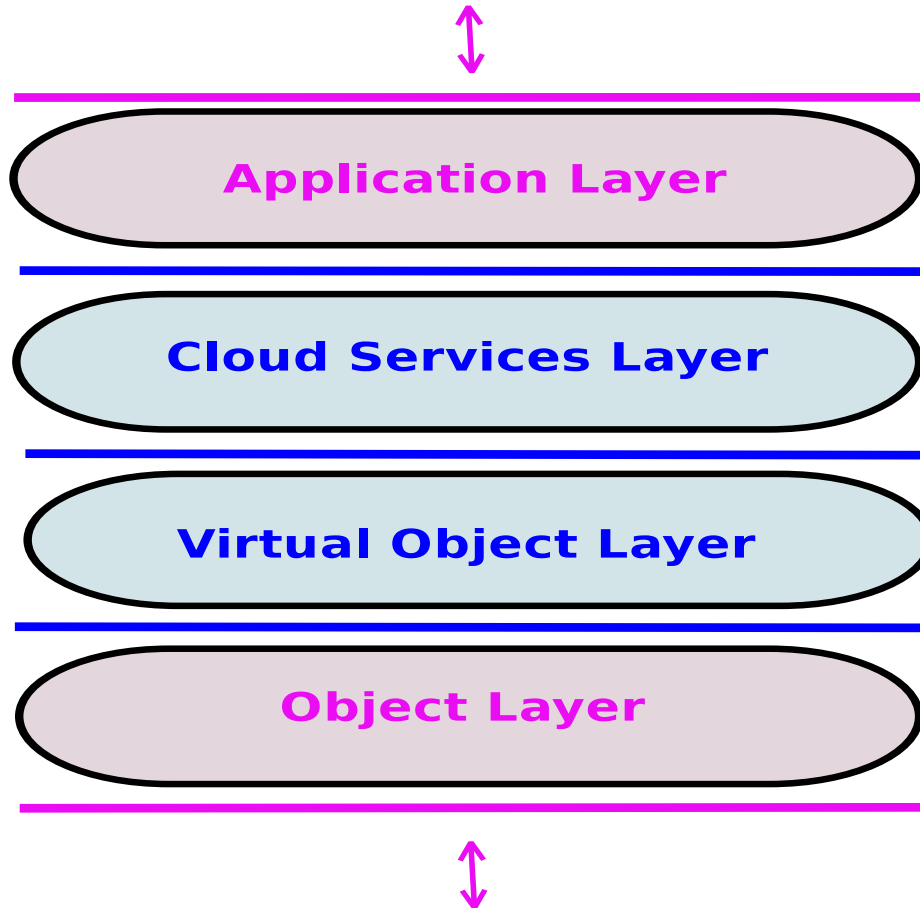


➤ Hierarchical Group and Attribute Based Access Control (HGABAC)

- ❖ Introduces User and Object Groups
- ❖ Simplifies administration of attributes

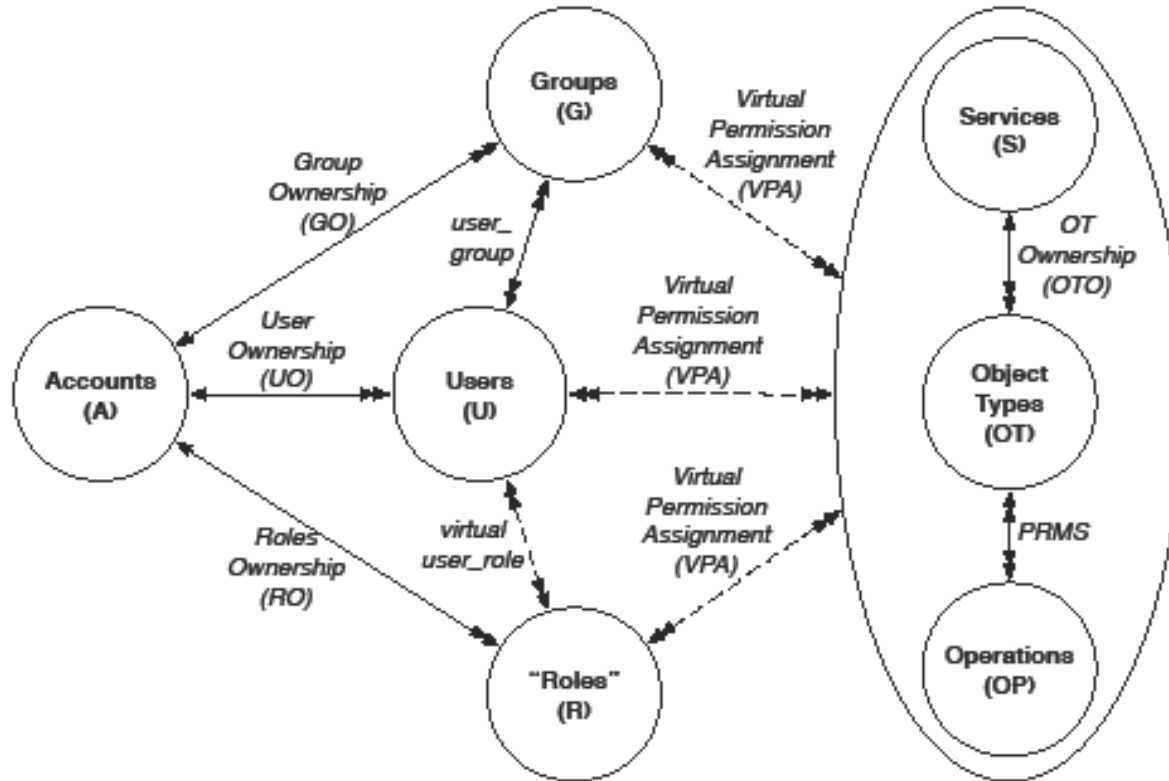
Servos and Osborn, 2015

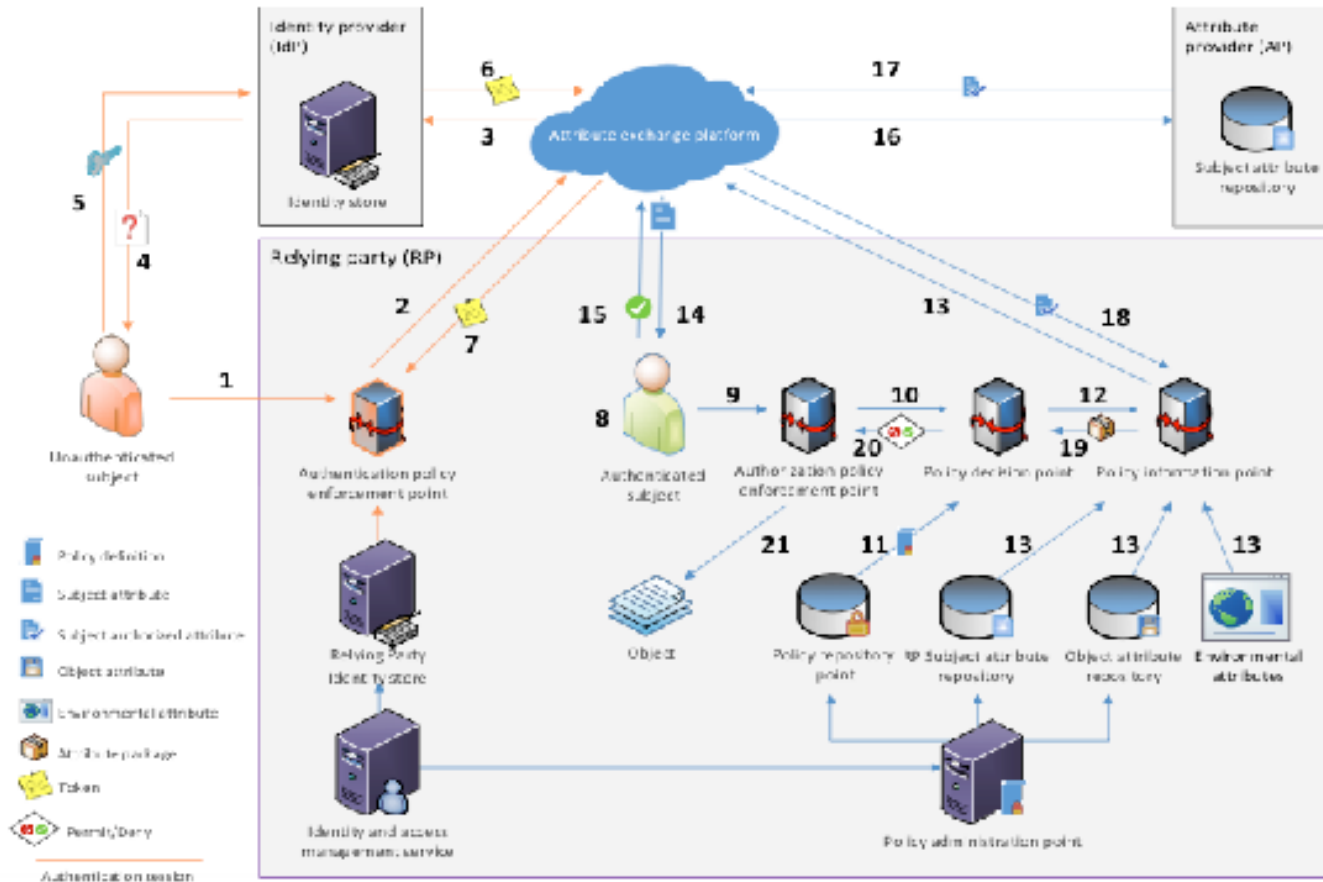
User and Administrator Interaction



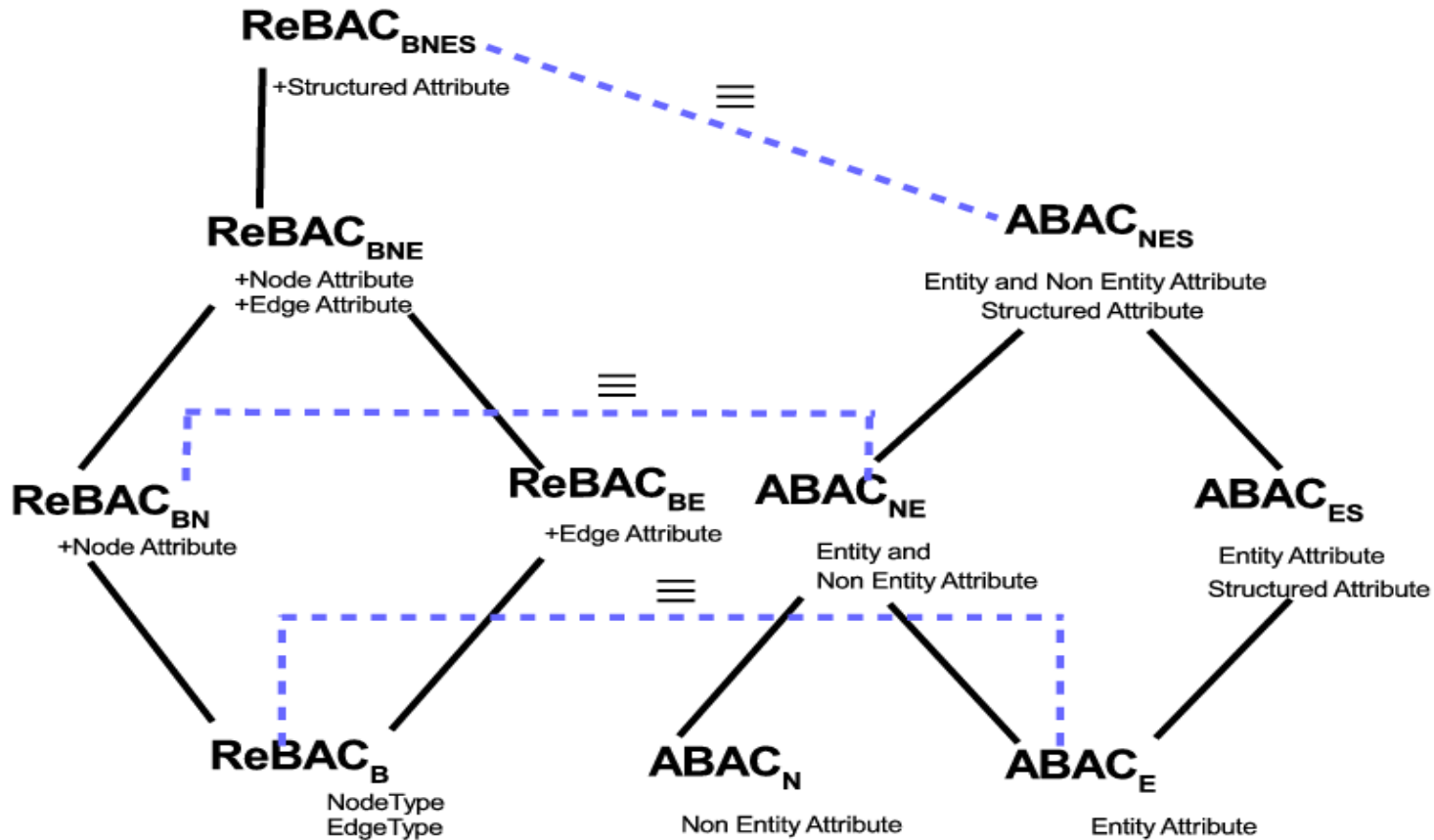
User Direct Interaction

Alsheri, Bhatt, Patwa,
Benson, Sandhu
2016 onwards





Fisher 2015
NCCOE, NIST, Building Block



**ReBAC and ABAC are not that different
(Tahmina, Sandhu 2017)**

**Discretionary Access Control
(DAC), 1970**

**Mandatory Access Control (MAC),
1970**

**Role Based Access Control
(RBAC), 1995**

**Attribute Based Access Control
(ABAC), ????**

Can subject *s* obtain a
right *r* on object *o*?
❖ Current state?
❖ Some future state?

**Safety
Complexity**

Ahmed, Rajkumar, Sandhu
2016 onwards