Module 4.2
Attribute-Based Access Control (ABAC)

Ravi Sandhu

Spring 2021
Access Control Models

Discretionary Access Control (DAC) 1970

Mandatory Access Control (MAC) 1970

Role Based Access Control (RBAC) 1995

Attribute Based Access Control (ABAC) 2020s (Hopefully)

Fixed policy

Flexible policy

World-Leading Research with Real-World Impact!

© Ravi Sandhu
Access Control Models

Discretionary Access Control (DAC) 1970

Fixed policy

Mandatory Access Control (MAC) 1970

Flexible policy

Role Based Access Control (RBAC) 1995

Access decision triple (s,o,r)
Fixed decision rule

Attribute Based Access Control (ABAC) 2020s (Hopefully)

Access decision quad (s,o,r,c)
Flexible decision rule
ABAC Decision Quad (s,o,r,c)

Computed based on attributes of s, o, r, c
Via customized rules

Subject s → Right r → Access Decision? Yes/No → Context c → Object o
Compare DAC, MAC, RBAC triple \((s,o,r)\)

Computed via fixed rules:
- DAC: \(s:r \in ACL(o)\)
- MAC: BLP rules
- RBAC: \(s\) has an active role that authorizes \(o,r\)
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
Operational model

- specify the decision function for the access decision triple or quad

Administrative

- specify the model’s dynamics
- dynamics change the system state and modify the outcome of some access decision triple or quads

Our ABAC focus

DAC, RBAC, ABAC ...
ABAC is not New

User (Identity)

Attributes

Public-key Certificate + Secured secrets
ABAC is not New

Pre Internet, early 1990s
ABAC is not New

Post Internet, late 1990s
ABAC is not New

User (Identity)

Attributes

SPKI Certificates

Public-keys + Secured secrets

Post Internet, late 1990s
ABAC is not New

Mature Internet, 2000s

User (Identity)

Anonymous Credentials

Attributes

Public-keys + Secured secrets
ABAC is not New

Attributes

- Action
- User
- Subject
- Object
- Context
- Policy

Authorization Decision

Yes/No

XACML

Mature Internet, 2000s
ABAC Policy Configuration

1. Constraints on subject attribute at creation and modification time
   (Different policies can be specified for creation and modification time)

2. Constraints on object attributes at creation and modification time
   ((Different policies can be specified for creation and modification time)

3. Authorization policy

U: User
S: Subject
O: Object
C: Context
P: Policy

Constraints → Association ← Creator
ABAC Policy Configuration

Can be configured to do many variations of DAC, MAC, RBAC
Access Control Models

Discretionary Access Control (DAC) 1970

Mandatory Access Control (MAC) 1970

Role Based Access Control (RBAC) 1995

Attribute Based Access Control (ABAC) 2020s (Hopefully)

Fixed policy

Flexible policy

© Ravi Sandhu
Access Control Models

Discretionary Access Control (DAC) 1970

Mandatory Access Control (MAC) 1970

Role Based Access Control (RBAC) 1995

Attribute Based Access Control (ABAC)

Encompasses

- Relationship-Based Access Control (ReBAC)
- Usage Control (UCON)
- Rule-Based, Policy-Based, etc

2020s (Hopefully)
Access Control Convergence

ABAC  ReBAC  RBAC  DAC  MAC

Convergent Access Control (CAC)

Access Control Policy Models  Access Control Enforcement Models

Application Context