Attribute-Based Access Control (ABAC)

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 10

ravi.utsa@gmail.com
www.profsandhu.com
Access Control

Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

Attribute Based Access Control (ABAC), ???
RBAC Shortcomings

- Constraints
- Impossible
- Hard Enough

© Ravi Sandhu

World-Leading Research with Real-World Impact!
The RBAC Story

ABAC Status

Pre-RBAC  Early RBAC  1st expansion phase  2nd expansion phase

1990?  2017

ABAC still in pre/early phase

© Ravi Sandhu

World-Leading Research with Real-World Impact!
ABAC is not New

User (Identity)

Attributes

Public-keys +
Secured secrets
ABAC is not New

Pre Internet, early 1990s
ABAC is not New

User (Identity)

X.509 Attribute Certificates

X.509 Identity Certificates

Attributes

Public-keys + Secured secrets

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

User (Identity)

Attributes

Anonymous Credentials

Public-keys + Secured secrets

Mature Internet, 2000s
ABAC is not New

Attributes

Authorization Decision

Yes/No

Mature Internet, 2000s

© Ravi Sandhu
ABAC$\alpha$ and ABAC$\beta$ Models
ABACα Model Structure

Policy Configuration Points

1. Constraints on subject attributes at creation and modification time.
2. Constraints on object attributes at creation and modification time.
3. Authorization policy

Just sufficient mechanism to do simple forms of DAC, MAC, RBAC
ABAC α Authorization Policy

- **DAC**
  \[\text{Authorization}_{\text{read}}(s, o) \equiv \text{SubCreator}(s) \in \text{reader}(o)\]
  \[\text{Authorization}_{\text{write}}(s, o) \equiv \text{SubCreator}(s) \in \text{writer}(o)\]

  \[\text{Authorization}_{\text{read}}(s, o) \equiv \text{sensitivity}(o) \leq \text{sclearance}(s)\]

- **MAC**
  Liberal star: \[\text{Authorization}_{\text{write}}(s, o) \equiv \text{sclearance}(s) \leq \text{sensitivity}(o)\]
  Strict star: \[\text{Authorization}_{\text{write}}(s, o) \equiv \text{sensitivity}(o) = \text{sclearance}(s)\]

- **RBAC0**
  \[\text{Authorization}_{\text{read}}(s, o) \equiv \exists r \in \text{srole}(s), r \in \text{rrole}(o)\]

- **RBAC1**
  \[\text{Authorization}_{\text{read}}(s, o) \equiv \exists r1 \in \text{srole}(s), \exists r2 \in \text{rrole}(o), r2 \leq r1\]
ABACα Subject Attribute Constraints

- **MAC creation**
  \[ \text{ConstrSub}(u, s, \{(sclearance, value)\}) \equiv \text{value} \leq \text{uclearance}(u) \]

- **RBAC0**
  \[ \text{ConstrSub}(u, s, \{srole, value\}) \equiv \text{value} \subseteq \text{urole}(u) \]

- **RBAC1**
  \[ \text{ConstrSub}(u, s, \{srole, value\}) \equiv \forall r_1 \in \text{value}. \exists r_2 \in \text{urole}(u). r_1 \leq r_2 \]
ABACα Object Attribute Constraints

- **DAC Creation**
  \[ ConstrObj(s, o, \{(reader, val1), (writer, val2), (createdby, val3)\}) \equiv val3 = SubCreator(s) \]

- **Modification**
  \[ ConstrObj(s, o, \{(reader, val1), (writer, val2), (createdby, val3)\}) \equiv createdby(o) = SubCreator(s) \]

- **MAC Creation**
  \[ ConstrObj(s, o, \{sensitivity, value\}) \equiv sclearance(s) \leq value \]

- **Modification**
  FALSE
Can be configured to do many but not all RBAC extensions
Roles and Attributes
Roles and Attributes

Attribute-Centric

Role is just another attribute. Nothing special about it.

Dynamic Roles

Compute user roles from user attributes

Role-Centric

Attributes constrain permissions of roles for each user
User-Role Assignment Problem

(RH) Role Hierarchy

(UA) User Assignment

(PA) Permission Assignment

Constraints

© Ravi Sandhu
Beyond Attributes
Access Control

Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

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

Relationship Based Access Control (ReBAC), 2008

Flexible policy

Fixed policy
Access Control

Fixed policy

Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Relationship Based Access Control (ReBAC), 2008

Role Based Access Control (RBAC), 1995

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

Flexible policy