Attribute-Based Access Control: Insights and Challenges

Prof. Ravi Sandhu
Executive Director and Endowed Chair

DBSec
Taipei, Taiwan
August 8, 2017

ravi.sandhu@utsa.edu
www.profsandhu.com
www.ics.utsa.edu
Policy-Mechanism

Policy

What?

Mechanism

How?
Access Control Evolution

Discretionary Access Control (DAC), 1970

Role Based Access Control (RBAC), 1995

Mandatory Access Control (MAC), 1970

Attribute Based Access Control (ABAC), ????
Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

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

Born 1990s
NO!! Never!!

Is ABAC the right word for the moment?
- Certainly a strong candidate
- Already too late?
  - ReBAC (relationship-based access control) not ABAC
  - Big Data, Analytics and AI will take care of everything

What is lacking in ABAC?
- Usage Control (UCON) concepts of attribute mutability, enforcement and obligation continuity, and post-obligations
- Task-Based Access Control
- Risk-Based Access Control
- Policy-Based Access Control
- ................
ABAC is orders of magnitude more complex than anything that has been an Access Control winner so far (DAC, MAC, RBAC)

- We need the complexity, but need to manage it
- If Google can index the web, we can do ABAC!!

Cloud-enabled IoT may be the killer app
ABAC Research Agenda

1. Foundational Principles and Theory
2. Core ABAC Models
3. Administrative ABAC Models
4. Extended ABAC Models
5. ABAC Policy Architectures and Languages
6. ABAC Enforcement Architectures
7. ABAC Design, Engineering and Applications

Based on RBAC experience
ABAC Research Agenda

1. Foundational Principles and Theory

2. Core ABAC Models

3. Administrative ABAC Models

4. Extended ABAC Models

5. ABAC Policy Architectures and Languages

6. ABAC Enforcement Architectures

7. ABAC Design, Engineering and Applications
2. Core ABAC Models: $\text{ABAC}_\alpha$

*Policy Configuration Points*

Can be configured to do simple forms of DAC, MAC, RBAC

Jin, Krishnan, Sandhu 2012
2. Core ABAC Models: $\text{ABAC}_\beta$

Can further be configured to do many
RBAC extensions
Jin, Krishnan, Sandhu 2014
Hierarchical Group and Attribute Based Access Control (HGABAC)

- Introduces the notion of User and Object Groups
- Core advantage is simplified administration of attributes
- User and Objects are assigned set of attributes in one go as compared to single assignment at a time.

Servos and Osborn, 2015
ABAC Research Agenda

1. Foundational Principles and Theory

2. Core ABAC Models

3. Administrative ABAC Models

4. Extended ABAC Models

5. ABAC Policy Architectures and Languages

6. ABAC Enforcement Architectures

7. ABAC Design, Engineering and Applications
3. Administrative ABAC Models: GURA and GURA\textsubscript{G}

![Diagram of ABAC models]

**Administrative Relations**

- **User Attribute Assignment (UAA) & User-Group Attribute Assignment (UGAA):**
  
  For each \( \text{att}_u \) in UA,
  
  \[
  \text{canAdd}_{\text{att}_u} \subseteq \text{AR} \times \text{EXPR(UA)} \times 2^{\text{Range}(\text{att}_u)}
  \]
  
  \[
  \text{canDelete}_{\text{att}_u} \subseteq \text{AR} \times \text{EXPR(UA)} \times 2^{\text{Range}(\text{att}_u)}
  \]

- **User to User-Group Assignment (UGA):**
  
  \[
  \text{canAssign} \subseteq \text{AR} \times \text{EXPR(UA} \cup \text{UG)} \times 2^{\text{UG}}
  \]
  
  \[
  \text{canRemove} \subseteq \text{AR} \times \text{EXPR(UA} \cup \text{UG)} \times 2^{\text{UG}}
  \]

Jin, Krishnan, Sandhu, 2012
Gupta, Sandhu, 2016
ABAC Research Agenda

1. Foundational Principles and Theory
2. Core ABAC Models
3. Administrative ABAC Models
4. Extended ABAC Models
5. ABAC Policy Architectures and Languages
6. ABAC Enforcement Architectures
7. ABAC Design, Engineering and Applications
4. Extended ABAC Models: UCON

- unified model integrating
  - authorization
  - obligation
  - conditions
- and incorporating
  - continuity of decisions
  - mutability of attributes

Usage Control Models, early 2000s
Park, Sandhu, Pretschner

© Ravi Sandhu
World-Leading Research with Real-World Impact!
4. Extended ABAC Models: ReBAC versus ABAC

Equivalence of ReBAC and ABAC Structural Variants
4. Extended ABAC Models: ReBAC versus ABAC

Non-Equivalence of ReBAC and ABAC Variants
ABAC Research Agenda

1. Foundational Principles and Theory

2. Core ABAC Models

3. Administrative ABAC Models

4. Extended ABAC Models

5. ABAC Policy Architectures and Languages

6. ABAC Enforcement Architectures

7. ABAC Design, Engineering and Applications
1. Foundations: Safety

- A single infinite attribute with no creation leads to undecidable safety. Rajkumar 2012
- Pre_UCON with finite attributes and unbounded creation has decidable safety. Rajkumar, Sandhu 2016
- ABAC_\alpha has decidable safety. Ahmed, Sandhu 2017
- GURA has decidable safety/reachability. Jin, Krishnan, Sandhu 2017
ABAC Research Agenda

1. Foundational Principles and Theory
2. Core ABAC Models
3. Administrative ABAC Models
4. Extended ABAC Models
5. ABAC Policy Architectures and Languages
6. ABAC Enforcement Architectures
7. ABAC Design, Engineering and Applications
5. Policy Architecture: Centralized ABAC$_{\alpha}$ style

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

Constraints
Association
Creator
5. Policy Architecture: Diffused AWS style
ABAC Research Agenda

1. Foundational Principles and Theory

2. Core ABAC Models

3. Administrative ABAC Models

4. Extended ABAC Models

5. ABAC Policy Architectures and Languages

6. ABAC Enforcement Architectures

7. ABAC Design, Engineering and Applications
6. ABAC Enforcement Architecture: Federated ABAC

Fisher 2015
NCCOE, NIST, Building Block
ABAC Research Agenda

1. Foundational Principles and Theory

2. Core ABAC Models

3. Administrative ABAC Models

4. Extended ABAC Models

5. ABAC Policy Architectures and Languages

6. ABAC Enforcement Architectures

7. ABAC Design, Engineering and Applications
7. ABAC Applications: Cloud IaaS

- Cloud Computing IaaS
  - Single tenant
  - Multi tenant
  - Multi cloud

Jin, Tang, Dang, Bijon, Pustchi, Zhang, Biswas, Ahmed, Cheng, Patwa, Krishnan, Sandhu
2012 onwards
7. ABAC Applications: Cloud Enabled IoT

User and Administrator Interaction

Application Layer

Cloud Services Layer

Virtual Object Layer

Object Layer

User Direct Interaction

Alsheri, Bhatt, Patwa, Benson, Sandhu
2016 onwards
ABAC Research Agenda

5. ABAC Policy Architectures and Languages

3. Administrative ABAC Models

4. Extended ABAC Models

2. Core ABAC Models

6. ABAC Enforcement Architectures

7. ABAC Design, Engineering and Applications

1. Foundational Principles and Theory