The Authorization Leap from Rights to Attributes: Maturation or Chaos?

Prof. Ravi Sandhu
Executive Director and Endowed Chair

PST
July 16, 2012

ravi.sandhu@utsa.edu
www.profsandhu.com
www.ics.utsa.edu
The Authorization Leap from Rights to Attributes:

Maturation or Chaos?

Messy or Chaotic?

Prof. Ravi Sandhu
Executive Director and Endowed Chair

PST
July 16, 2012

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

© Ravi Sandhu
World-Leading Research with Real-World Impact!
Prognosis: Cyberspace

- Cyberspace will become orders of magnitude more complex and confused very quickly.

- Overall this is a very positive development and will enrich human society.

- It will be messy but need not be chaotic!
Discretionary Access Control (DAC), 1970

Role Based Access Control (RBAC), 1995

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

Fixed policy

Discretionary Access Control (DAC), 1970

Role Based Access Control (RBAC), 1995

Attribute Based Access Control (ABAC), 1995

Flexible policy

Mandatory Access Control (MAC), 1970
Prognosis: Access Control

Discretionary Access Control (DAC), 1970

Role Based Access Control (RBAC), 1995

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

Mandatory Access Control (MAC), 1970

Fixed policy

Flexible policy

Messy or Chaotic?
Access Control Limitations

- Analog Hole
- Inference
- Covert Channels
- Side Channels
- Phishing
- Safety
- Usability
- Privacy
- Attack Asymmetry
- Compatibility
- Federation
- ...
Access Control Limitations

- Analog Hole
- Inference
- Covert Channels
- Side Channels
- Phishing
- Safety
- Usability
- Privacy
- Attack Asymmetry
- Compatibility
- Federation

Can manage
Cannot eliminate
Access Control Models

- Discretionary Access Control (DAC), 1970
  - Owner controls access
  - But only to the original, not to copies
  - Grounded in pre-computer policies of researchers

- Mandatory Access Control (MAC), 1970
  - Synonymous to Lattice-Based Access Control (LBAC)
  - Access based on security labels
  - Labels propagate to copies
  - Grounded in pre-computer military and national security policies

- Role-Based Access Control (RBAC), 1995
  - Access based on roles
  - Can be configured to do DAC or MAC
  - Grounded in pre-computer enterprise policies

Numerous other models but only 3 successes: SO FAR
The RBAC Story

NIST-ANSI Standard Proposed

NIST-ANSI Standard Adopted

Year of Publication

Amount of Publications

Pre-RBAC  Early RBAC  2nd expansion phase

© Ravi Sandhu  World-Leading Research with Real-World Impact!
RBAC96 Model

(RH)
Role Hierarchy

(UA)
User Assignment

(PA)
Permission Assignment

Constraints

© Ravi Sandhu

World-Leading Research with Real-World Impact!
RBAC can be configured to do MAC
RBAC can be configured to do DAC
RBAC is policy neutral

RBAC is neither MAC nor DAC!
RBAC Shortcomings

- Role granularity is not adequate leading to role explosion
  - Researchers have suggested several extensions such as parameterized privileges, role templates, parameterized roles (1997-)
- Role design and engineering is difficult and expensive
  - Substantial research on role engineering top down or bottom up (1996-), and on role mining (2003-)
- Assignment of users/permissions to roles is cumbersome
  - Researchers have investigated decentralized administration (1997-), attribute-based implicit user-role assignment (2002-), role-delegation (2000-), role-based trust management (2003-), attribute-based implicit permission-role assignment (2012-)
- Adjustment based on local/global situational factors is difficult
  - Temporal (2001-) and spatial (2005-) extensions to RBAC proposed
- RBAC does not offer an extension framework
  - Every shortcoming seems to need a custom extension
  - Can ABAC unify these extensions in a common open-ended framework?
**RBAC Policy Configuration Points**

**Role Hierarchy (RH)**

- **Security Administrator**
- **User**
- **Session**
- **Role**
- **OPS**
- **OBS**

**User Assignment (UA)**

**Permission Assignment (PA)**

**Constraints**

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Access Control Models

Policy Specification

Policy Reality

Policy Enforcement

RBAC, ABAC
Initial focus

MAC, DAC
focus

Policy Administration

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Attribute-Based Access Control (ABAC)

- Attributes are name:value pairs
  - possibly chained
  - values can be complex data structures

- Associated with
  - users
  - subjects
  - objects
  - contexts
    - device, connection, location, environment, system …

- Converted by policies into rights just in time
  - policies specified by security architects
  - attributes maintained by security administrators
  - ordinary users morph into architects and administrators

- Inherently extensible
ABAC Status

1990?
ABAC still in pre/early phase

2012

Year of Publication

Amount of Publications

Pre-RBAC Early RBAC 2nd expansion phase

© Ravi Sandhu

World-Leading Research with Real-World Impact!
ABAC Prior Work Includes

- X.509, SPKI Attribute Certificates (1999 onwards)
  - IETF RFCs and drafts
  - Tightly coupled with PKI (Public-Key Infrastructure)
- XACML (2003 onwards)
  - OASIS standard
  - Narrowly focused on particular policy combination issues
  - Fails to accommodate the ANSI-NIST RBAC standard model
  - Fails to address user subject mapping
- Usage Control or UCON (Park-Sandhu 2004)
  - Fails to address user subject mapping
  - Focus is on extended features
    - Mutable attributes
    - Continuous enforcement
    - Obligations
    - Conditions
- Several others ………..
An ABAC model requires
- identification of policy configuration points (PCPs)
- languages and formalisms for each PCP

A core set of PCPs can be discovered by building the ABACα model to unify DAC, MAC and RBAC

Additional ABAC models can then be developed by
- increasing the sophistication of the ABACα PCPs
- discovering additional PCPs driven by requirements beyond DAC, MAC and RBAC

A small but crucial step
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

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Authorization Policy: LAuthorization

**DAC**

\[ Authorization_{read}(s, o) \equiv SubCreator(s) \in reader(o) \]
\[ Authorization_{write}(s, o) \equiv SubCreator(s) \in writer(o) \]

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

**MAC**

Liberal star: \[ Authorization_{write}(s, o) \equiv \text{sclearance}(s) \leq \text{sensitivity}(o) \]

Strict star: \[ Authorization_{write}(s, o) \equiv \text{sensitivity}(o) = \text{sclearance}(s) \]

**RBAC0**

\[ Authorization_{read}(s, o) \equiv \exists r \in srole(s). r \in rrole(o) \]

**RBAC1**

\[ Authorization_{read}(s, o) \equiv \exists r1 \in srole(s). \exists r2 \in rrole(o). r2 \leq r1 \]
Subject Attribute Constraints; LConstrSub

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

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

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

Constraints at creation: LConstrObj

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

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

Constraints at modification: LConstrObjMod

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

Future work
- increasing the sophistication of the ABACα PCPs
- discovering additional PCPs
ABAC Research Agenda

7. ABAC Design and Engineering

5. ABAC Policy Languages

3. Administrative ABAC Models

4. Extended ABAC Models

2. Core ABAC Models

6. ABAC Enforcement Architectures

1. Foundational Principles and Theory
# ABAC Research Agenda

## 1. Foundational Principles and Theory

## 2. Core ABAC Models
- Initial Results

## 3. Administrative ABAC Models

## 4. Extended ABAC Models

## 5. ABAC Policy Languages

## 6. ABAC Enforcement Architectures

## 7. ABAC Design and Engineering
7. Design and Engineering:

5. Policy Languages


1. Foundational Principles and Theory


NOTE: Only a small sampling of the RBAC literature is cited in this diagram

© Ravi Sandhu
World-Leading Research with Real-World Impact!
Authorization Leap

Rights to attributes
- Rights
- Labels
- Roles
- Attributes

Benefits
- Decentralized
- Dynamic
- Contextual
- Consolidated

Risks
- Complexity
- Confusion
- Attribute trust
- Policy trust

Messy ☹️ Chaotic