Attribute-Based Access Control Models and Beyond

Prof. Ravi Sandhu

Executive Director, Institute for Cyber Security
Lutcher Brown Endowed Chair in Cyber Security
University of Texas at San Antonio

Cybersecurity Lecture Series
CIC 2015, Hangzhou, China
Oct 29, 2015

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

v2.0
Access Control

Discretionary Access Control (DAC), 1970

Role Based Access Control (RBAC), 1995

Mandatory Access Control (MAC), 1970

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

Security and system goals (objectives/policy)

Policy models

Enforcement models

Implementation models

Trusted Computing Technology (mechanisms/implementation)

Necessarily Informal

Formal/quasi-formal

System block diagrams, Protocol flows

Pseudo-code

Actual Code

Idealized

Enforceable (Approximate)

Codeable
Access Control

Discretionary Access Control (DAC), 1970

Role Based Access Control (RBAC), 1995

Mandatory Access Control (MAC), 1970

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

Discretionary Access Control (DAC), 1970

Role Based Access Control (RBAC), 1995

Mandatory Access Control (MAC), 1970

Attribute Based Access Control (ABAC), ???

Fixed policy

Flexible policy
Access Control

- Discretionary Access Control (DAC), 1970
- Mandatory Access Control (MAC), 1970
- Role Based Access Control (RBAC), 1995
- Attribute Based Access Control (ABAC), ????

Enterprise Oriented

Beyond Enterprise
Access Control

Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

Attribute Based Access Control (ABAC), ????
RBAC96 Model

(RH) Role Hierarchy

(UA) User Assignment

(PA) Permission Assignment

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Fundamental Theorem of RBAC

- 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

Hard Enough

 Impossible

(Role Hierarchy)

(User Assignment)

(Permission Assignment)

Constraints

© Ravi Sandhu

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

NIST-ANSI Standard Proposed

NIST-ANSI Standard Adopted

Amount of Publications

Year of Publication

3 2 7 3 28 30 30 35 40 48 53 88 85 88 112 103 111 866

RBAC96 model

ABAC Status

ABAC still in pre/early phase

1990?

2015
ABAC is not New

User (Identity)

Attributes

Public-keys + Secured secrets
ABAC is not New

X.500 Directory

Attributes

User (Identity)

X.509 Identity Certificates

Public-keys + Secured secrets

Pre Internet, early 1990s
ABAC is not New

User (Identity)

X.509 Attribute Certificates

Attributes

Public-keys + Secured secrets

X.509 Identity Certificates

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

Action →
User →
Subject →
Object →
Context →
Policy → Authorization Decision → Yes/No → XACML

Mature Internet, 2000s
ABAC is not New

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

Usage Control Models, early 2000s

- Rights (R)
- Permissions (P)
- Obligations (O)
- Conditions (C)
- Subj ect Attributes (SA)
- Object Attributes (OA)
ABAC Status

1990? 2015

ABAC still in pre/early phase


Proposed Standard
Standard Adopted

Amount of Publications

Year of Publication

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

© Ravi Sandhu

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

Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

Attribute Based Access Control (ABAC), ????
ABACα Model Structure

Can be configured to do simple forms of DAC, MAC, RBAC
1. Context Attributes

2. Subject attribute constraints policy are different at creation and modification time.

3. Subject attributes constrained by attributes of subjects created by the same user.

4. Policy Language

5. Meta-Attributes

Extended Constraints on Role Activation:

1, 2, 4, 5

Extended Concept of Role:
Role Template-1997 [45], Parameterized RBAC-2004 [2], Parameterized RBAC-2003 [34], Parameterized Role-2004 [43], Attributed Role-2006 [99]

2, 4

Changes in Role-Permission Relationship:
Task-RBAC-2000 [77], Task-RBAC-2003 [78]

4, 5

Extended Permission Structure:
RBAC with Object class- 2007 [24], Conditional PRBAC 07 [74], PRBAC 07 [75], Purpose-aware RBAC- 2008 [67], Ubi-RBAC-2010 [76], RCPBAC-2011 [55]

1, 2, 3, 4, 5

Organization and Team:
Can be configured to do many RBAC extensions
SOME RESEARCH CHALLENGES
Ultimate Unified Model

Attributes

Security
Access Control
Trust
Risk

Relationships

Provenance
Expressive Power

- Security and system goals (objectives/policy)
  - Necessarily informal
  - Formal/quasi-formal

- Policy models
  - Vertical view
  - Looks across layers

- Enforcement models
  - Horizontal view
  - Looks at individual layer

- Implementation models
  - System block diagrams, protocol flows
  - Pseudo-code
  - Actual code

- Trusted Computing Technology (mechanisms/implementation)

Idealized
Enforceable (Approximate)
Codeable
Safety Analysis

Idealized

Enforceable (Approximate)

Codeable
Attribute and Policy Engineering

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

Constraints → Association ← Creator
Application Domains

- Cloud computing
- Internet of Things
Access Control

Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

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