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
Austrian Institute of Technology (AIT) and TU Vienna
June 3, 2015

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

v2.0

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), ???
PEI Models

Security and system goals (objectives/policy)

Policy models

Necessarily Informal

Formal/quasi-formal

System block diagrams, Protocol flows

Pseudo-code

Actual Code

Enforcement models

Idealized

Enforceable

(Approximate)

Implementation models

Vertical view

Looks Across Layers

Trusted Computing Technology (mechanisms/implementation)

Horizontal view

Looks at Individual layer

Vertical View

Looks Across Layers

World-Leading Research with Real-World Impact!

© Ravi Sandhu
Access Control

Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

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

Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

Attribute Based Access Control (ABAC), ???

Fixed policy

Flexible policy
Access Control

Discretionary Access Control (DAC), 1970

Role Based Access Control (RBAC), 1995

Attribute Based Access Control (ABAC), ???

Mandatory Access Control (MAC), 1970

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

Constraints

© 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

(RH)
Role Hierarchy

(UA)
User Assignment

(PA)
Permission Assignment

(OPS)

(OBS)

PRMS

Constraints

© Ravi Sandhu

World-Leading Research with Real-World Impact!
ABAC Status

1990?

ABAC still in pre/early phase


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

Attributes

X.509 Attribute Certificates

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

Mature Internet, 2000s

User (Identity)

Attributes

Anonymous Credentials

Public-keys + Secured secrets
ABAC is not New

Attributes

Authorization Decision

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

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
ABAC Status

- **1st expansion phase**: 1995-2000
- **2nd expansion phase**: 2005-2008
- **Pre-RBAC**: 1990?
- **Early RBAC**: 2015
- **ABAC still in pre/early phase**: 2015

Years:
- 1992: 3
- 1995: 2
- 1996: 7
- 2000: 18
- 2005: 50
- 2008: 88

Additional data:
- **RBAC96 paper**: 1996
- **Proposed Standard**: 1998
- **Standard Adopted**: 2000
- **Total Publications**: 866

© Ravi Sandhu  
*World-Leading Research with Real-World Impact!*
Access Control

Discretionary Access Control (DAC), 1970

Role Based Access Control (RBAC), 1995

Mandatory Access Control (MAC), 1970

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

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

© Ravi Sandhu

World-Leading Research with Real-World Impact!
RBAC Extensions

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:

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

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

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]
ABAC_{\beta} Model

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

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)

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
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
- ..........

© 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), ???