Security Limitations

- Analog Hole
- Inference
- Covert Channels
- Side Channels
- Phishing
- Social Engineering
- Attack Asymmetry
- Privacy vs Security
- Base-rate Fallacy
- ...
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

Administration Driven
Automated Adaptive

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

Enterprise Oriented

Discretionary Access Control (DAC), 1970

Role Based Access Control (RBAC), 1995

Mandatory Access Control (MAC), 1970

Attribute Based Access Control (ABAC), ???

Beyond Enterprise
Access Control

Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

Messy or Chaotic?

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

Policy Specification

Policy Reality

Policy Enforcement

- RBAC, ABAC
  Initial focus

- RBAC, ABAC
  Next step focus

- MAC, DAC
  Main focus

- MAC, DAC
  Easy (relatively)
The RBAC Story

Amount of Publications

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

RBAC96 Model

Role Hierarchy

Constraints

© Ravi Sandhu

World-Leading Research with Real-World Impact!
RBAC Policy Configuration Points

Security Architect

Role Hierarchy

Security Administrator

Security Administrator

USER

ROLES

USER ASSIGNMENT

Permission Assignment

( RH )

( UA )

( PA )

Constraints

Security Architect

Session Roles

Security Architect

Security Architect

Security Administrator

Security Administrator

© 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 Shortcomings

Hard Enough

Impossible

(RH) Role Hierarchy

(UA) User Assignment

(PA) Permission Assignment

OPS

OBS

PRMS

Constraints

© Ravi Sandhu

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

User (Identity)

Attributes

Public-keys + Secured secrets
ABAC is not New

User (Identity)

X.500 Directory

Attributes

Public-keys + Secured secrets

X.509 Identity Certificates

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

- Action
- User
- Subject
- Object
- Context
- Policy
ABAC is not New

Attributes

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

Authorization Decision

Yes/No

Usage Control
XACML
Attribute-Based Encryption

Mature Internet, 2000s
ABAC Status

Amount of Publications

Year of Publication

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

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

1990?  2014

ABAC still in pre/early phase

RBAC96 paper

Proposed Standard

Standard Adopted

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Attributes are name:value pairs
- possibly chained
- values can be complex data structures

Associated with
- actions
- users
- subjects
- objects
- contexts
- policies

Converted by policies into rights just in time
- policies specified by security architects
- attributes maintained by security administrators
- but also possibly by users OR reputation and trust mechanisms

Inherently extensible
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 simple forms of 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 first 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

Constraints → Association → Creator

© Ravi Sandhu
ABACα Model Structure

Policy Configuration Points

Can be configured to do 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
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

Constraints ➔ Association ➔ Creator
Beyond ABAC

Attributes
- Security
- Access Control
- Trust
- Risk

Relationships

Provenance
GURA model for user-attribute assignment
Safety analysis of ABAC\(_\alpha\) and ABAC\(_\beta\)
Undecidable safety for ABAC models
Decidable safety for ABAC with finite fixed attributes
Constraints in ABAC
ABAC Cloud IaaS implementations (OpenStack)
Attribute Engineering
Attribute Mining
Unification of Attributes, Relationships and Provenance