Access Control Convergence: Challenges and Opportunities

Ravi Sandhu
Executive Director and Chief Scientist
Professor of Computer Science
Lutcher Brown Chair in Cyber Security

Ontario Tech University, Canada
March 11 2021

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

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Convergent Research

Disciplinary

Multi-Disciplinary

Inter-Disciplinary

Convergent

INCREASED

Collaboration
Interaction
New paradigms
New concepts
New language
New disciplines
Convergent Research

Disciplinary

Multi-Disciplinary

Inter-Disciplinary

Convergent

INCREASED

Collaboration
Interaction
New paradigms
New concepts
New language
New disciplines

NAP = National Academies Press

NAP Report 2005

NAP Report 2014
Convergent Research

- Disciplinary
  - Multi-Disciplinary
  - Inter-Disciplinary
  - Cross-Disciplinary
  - Trans-Disciplinary

INCREASED
- Collaboration
- Interaction
- New paradigms
- New concepts
- New language
- New disciplines

World-Leading Research with Real-World Impact!
Convergent Research

Disciplinary

Multi-Disciplinary

Inter-Disciplinary

Convergent

INCREASED

Collaboration
Interaction
New paradigms
New concepts
New language
New disciplines

DRIVERS
-- Deep scientific questions
-- Pressing societal needs
Cyber Security Research Convergence

Objectives

Enable

Enforce

What?

Why?

Respond

Defend

Policy

Attacks

Mechanisms

Protect

Detect

Complement

How?

Application Context

World-Leading Research with Real-World Impact!
Cyber Security Research Convergence

Objectives

Policy

Attacks

Deep scientific questions:
-- We have no clue how to do this

Pressing societal need:
-- Cyber security is hugely important and broken
-- Cyber security researchers lack incentive to converge

Enforce

Enable

How?

Respond

Defend

Application

Context

Mechanisms

Protect

Detect

Complement

© Ravi Sandhu
Access Control Research Convergence

- ABAC
- ReBAC
- RBAC
- DAC
- MAC

Convergent Access Control (CAC)

Access Control Policy Models

Access Control Enforcement Models

Application Context
Deep scientific questions:
-- We have no clue how to do this
-- Will revisit at end of talk

Pressing societal need:
-- Cyber security is hugely important and broken
-- Access control is an essential piece to secure modern cyber applications: IoT, CPS, smart communities, ...
-- Cyber security researchers have no incentive to converge
-- Convergence may be easier in Access Control vs all of cyber security
Access Control Research Convergence

Convergent Access Control (CAC)

Access Control Policy Models ↔ Access Control Enforcement Models

- ABAC
- ReBAC
- RBAC
- DAC
- MAC
- ...
Access Control
PEI Layers

<table>
<thead>
<tr>
<th>Security and system goals (objectives/policy)</th>
<th>Necessarily Informal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy models</td>
<td>Formal/quasi-formal</td>
</tr>
<tr>
<td>Enforcement models</td>
<td>System block diagrams, Protocol flows</td>
</tr>
<tr>
<td>Implementation models</td>
<td>Pseudo-code</td>
</tr>
<tr>
<td>Trusted Computing Technology (mechanisms/implementation)</td>
<td>Actual Code</td>
</tr>
</tbody>
</table>

Big decisions
Idealized
Enforceable
Codeable
Code
Access Control
PEI Layers

Our focus

Security and system goals (objectives/policy)

Necessarily Informal

Formal/ quasi-formal

System block diagrams, Protocol flows

Pseudo-code

Actual Code

Policy models

Big decisions

Idealized

Enforceable

Codeable

Vertical view
Looks across layers

Enforcement models

Implementation models

Trusted Computing Technology (mechanisms/implementation)

Horizontal view
Looks at individual layer
Enforcement Models

PUSH MODEL

Client ➔ Server

Authentication + Authorization Credentials

PULL MODEL

Client ➔ Server

Authentication Credentials ➔ Authorization Credentials
Access Control
PEI Layers

Our focus

Security and system goals
(objectives/policy)

Necessarily
Informal

Formal/
quasi-formal

System block
diagrams,
Protocol flows

Pseudo-
code

Actual
Code

Policy models

Big decisions

Idealized

Enforceable

Codeable

Enforcement models

Implementation models

Trusted Computing Technology
(mechanisms/implementation)
Access Control

Discretionary Access Control (DAC) 1970

Mandatory Access Control (MAC) 1970

Role Based Access Control (RBAC) 1995

Attribute Based Access Control (ABAC)
Relationship-Based Access Control (ReBAC)
Usage Control (UCON)

2020s (Hopefully)
Discretionary Access Control (DAC)

- **Core concept:**
  Custodian of information determines access

- **Core drawback:**
  Does not protect copies
  Therefore OK for integrity but not for confidentiality

- **Sophistication:**
  Delegation of custody
  Denials or negative rights
Mandatory Access Control (MAC)

can-flow

Top Secret

Secret

Confidential

Unclassified
Mandatory Access Control (MAC)

- **Core concept:**
  Extend control to copies by means of security labels

- **Core drawback:**
  - Covert/side channels bypass MAC
  - Inference not prevented
  - Too strict
  - Too reductionist

- **Sophistication:**
  Dynamic labels
Access Control

Discretionary Access Control (DAC)  
1970

Mandatory Access Control (MAC)  
1970

Role Based Access Control (RBAC)  
1995

Attribute Based Access Control (ABAC)  
Relationship-Based Access Control (ReBAC)  
Usage Control (UCON)  
2020s (Hopefully)
Role-Based Access Control (RBAC)

- Core concept:
  Roles determine everything

- Core drawback:
  Roles are a natural concept for human users
  But not so natural for:
  Information objects
  IoT things
  Contextual attributes

- Sophistication:
  Role hierarchies
  Role constraints
Access Control

Discretionary Access Control (DAC) 1970

Mandatory Access Control (MAC) 1970

Role Based Access Control (RBAC) 1995

Attribute Based Access Control (ABAC)
Relationship-Based Access Control (ReBAC)
Usage Control (UCON)
2020s (Hopefully)
Attribute-Based Access Control (ABAC)

- Actor
- Context
- Operation
- Target

Access Decision? Yes/No
 Attribute-Based Access Control (ABAC)

- Core concept:
  Attributes determine everything
  No fixed access decision rule

- Core drawback:
  Flexibility at the cost of complexity

- Sophistication:
  Chained attributes
  Group attributes
  Distributed decision rules
  Automation
  Adaptation
Access Control

Discretionary Access Control (DAC) 1970

Mandatory Access Control (MAC) 1970

Role Based Access Control (RBAC) 1995

Attribute Based Access Control (ABAC)
Relationship-Based Access Control (ReBAC)
Usage Control (UCON)
2020s (Hopefully)
Rich set of building blocks:
DAC, MAC, RBAC, ABAC, ReBAC, UCON
We have some understanding of the relationships amongst these
Rich set of building blocks:
DAC, MAC, RBAC, ABAC, ReBAC, UCON
We have some understanding of the relationships amongst these

Do we need more building blocks?
We have very little understanding of synergy amongst these
Access Control: What Next?

- Rich set of building blocks: DAC, MAC, RBAC, ABAC, ReBAC, UCON
- We have some understanding of the relationships amongst these
- Do we need more building blocks?
- We have very little understanding of synergy amongst these

Deep scientific question for convergent research
Rich set of building blocks:
DAC, MAC, RBAC, ABAC, ReBAC, UCON

We have some understanding of the relationships amongst these

Do we need more building blocks?

We have very little understanding of synergy amongst these

Pressing societal need?

Deep scientific question for convergent research
Smart Communities

Integrated Community Cloud

Cloud-to-Cloud Data Transfer  IoT Devices Data Collections and Transmission  Relationships between Entities

Entities (e.g., Users and Devices) have attributes along with other environmental attributes and may have associated roles and capabilities in Smart Communities
Convergent Access Control (CAC)

Access Control Policy Models

Access Control Enforcement Models

ABAC
ReBAC
RBAC
DAC
MAC

Application Context