Safety of $\text{ABAC}_\alpha$ is Decidable

Tahmina Ahmed and Ravi Sandhu
Institute for Cyber Security and
Department of Computer Science

11th International Conference on
Network and System Security (NSS)

Helsinki, Finland
August 21-23, 2017

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

© Ahmed & Sandhu

World-Leading Research with Real-World Impact!
Can subject \( s \) obtain a right \( r \) on an object \( o \)?

- In current state?
- In some future state?
Access Control Evolution

Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

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

- Discretionary Access Control (DAC), 1970
- Mandatory Access Control (MAC), 1970
- Role Based Access Control (RBAC), 1995
- Attribute Based Access Control (ABAC), ????
Can be configured to do simple forms of DAC, MAC, RBAC
Jin, Krishnan, Sandhu 2012
ABAC_\alpha Model

Policy Configuration Points

Can be configured to do simple forms of DAC, MAC, RBAC
Jin, Krishnan, Sandhu 2012
ABAC_\alpha Model Components

- **Set of Users (U), Subjects (S) and Objects (O)**
- **Set of User Attributes (UA), Subject Attributes (SA) and Object Attributes (OA)**
- **Authorization Policy:**
  - Set of Permissions P
  - Authorization Policy $Authorization_p(s, o)$
- **Creation and Modification Policy:**
  - Subject Creation and Modification Constraint
  - Object Creation and Modification constraint

### Functional Specification
- $Access_p(s, o)$
- $CreateSubject(u, s, savt)$
- $ModifySubjectAtt(u, s, savt)$
- $DeleteSubject(u, s)$
- $CreateObject(s, o, oavt)$
- $ModifyObjectAtt(s, o, oavt)$

© Ahmed & Sandhu
Can subject s obtain a right r on an object o?

- Develop a safety algorithm specifically for ABAC$_\alpha$
- Reduce the safety problem for ABAC$_\alpha$ to the safety problem for some other ABAC model with known decidable safety
Can subject $s$ obtain a right $r$ on an object $o$?

- Develop a safety algorithm specifically for $ABAC_\alpha$

- Reduce the safety problem for $ABAC_\alpha$ to the safety problem for some other $ABAC$ model with known decidable safety
• unified model integrating
  • authorization
  • obligation
  • conditions
• and incorporating
  • continuity of decisions
  • mutability of attributes

Usage Control Models, early 2000s
Park, Sandhu, Pretschner

© Ahmed & Sandhu
• unified model integrating
  • authorization
  • obligation
  • conditions
• and incorporating
  • continuity of decisions
  • mutability of attributes

Usage Control Models, early 2000s
Park, Sandhu, Pretschner

© Ahmed & Sandhu

World-Leading Research with Real-World Impact!
Figure 4: $UCON^{finite}_{preA}$ Model
Object schema $OS_\Delta : \{a_1: \sigma_1 , ..., a_n: \sigma_n\}$

Usage Rights $UR: \{r_1, r_2, ..., r_k\}$:

Usage Control Commands $UC: \{uc_1, uc_2, ... uc_l\}$

Set of Attributes $ATT = \{a_1, a_2, ... a_n\}$

Set of Attribute Value tuples $AVT = \sigma_1 \times \sigma_2 \times \cdots \times \sigma_n$
**Non-Creating Command**

<table>
<thead>
<tr>
<th>Command Name ( r(s,o) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>PreCondition: ( f_b(s,o) \rightarrow {true, false} );</td>
</tr>
<tr>
<td>PreUpdate: ( s.a_{i_1} := f_{1,a_{i_1}}(s,o); )</td>
</tr>
<tr>
<td>:</td>
</tr>
<tr>
<td>( s.a_{i_p} := f_{1,a_{i_p}}(s,o); )</td>
</tr>
<tr>
<td>( o.a_{j_1} := f_{2,a_{j_1}}(s,o); )</td>
</tr>
<tr>
<td>:</td>
</tr>
<tr>
<td>( o.a_{j_q} := f_{2,a_{j_q}}(s,o); )</td>
</tr>
</tbody>
</table>

---

**Creating Command**

<table>
<thead>
<tr>
<th>Command Name ( r(s,o) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>PreCondition: ( f_b(s) \rightarrow {true, false} );</td>
</tr>
<tr>
<td>PreUpdate: create ( o; )</td>
</tr>
<tr>
<td>( s.a_{i_1} := f_{1,a_{i_1}}(s); )</td>
</tr>
<tr>
<td>:</td>
</tr>
<tr>
<td>( s.a_{i_p} := f_{1,a_{i_p}}(s); )</td>
</tr>
<tr>
<td>( o.a_{j_1} := f_{2,a_{j_1}}(s); )</td>
</tr>
<tr>
<td>:</td>
</tr>
<tr>
<td>( o.a_{j_q} := f_{2,a_{j_q}}(s); )</td>
</tr>
</tbody>
</table>
Entities: $ABAC_\alpha$ has users, subjects, objects as entities while $UCON_{finite}^{preA}$ has only subjects and objects as entities.

Attribute Mutability: Attributes of $ABAC_\alpha$ are Immutable while Attributes of $UCON_{finite}^{preA}$ is Mutable.

Operations: $ABAC_\alpha$ functions has configurable condition part and mandatory update part while $UCON_{finite}^{preA}$ has tightly coupled PreCondition part with optional Update part.
Shown in this paper:

- $\text{ABAC}_\alpha$ can be reduced to $\text{UCON}_{\text{finite}}^{\text{preA}}$
- Therefore $\text{ABAC}_\alpha$ has decidable safety

Open question:

- Can $\text{UCON}_{\text{preA}}^{\text{finite}}$ be reduced to $\text{ABAC}_\alpha$