Formal Verification of Usage Models: A Case Study of UseCON Using TLA+

Antonios Gouglidis\textsuperscript{1}  
\textsuperscript{1}School of Computing and Communications Lancaster University Lancaster, United Kingdom

Christos Grompanopoulos\textsuperscript{2}  
\textsuperscript{2}Department of Mechanical Engineering, University of Western Macedonia, Kozani, Greece

Anastasia Mavridou\textsuperscript{3}  
\textsuperscript{3}Institute for Software Integrated Systems, Vanderbilt University, Nashville, TN, USA

Satellite workshop of ETAPS 2018 — 15th of April 2018, Thessaloniki, Greece
Outline

• Motivation

• The UseCON model – specifications

• Verification and performance evaluation

• Discussion
Motivation – Access control

- Access Control Policies
- Access Control Models
- Access Control Mechanisms

DAC | MAC | RBAC | ABAC / UCON
Motivation - Verification

Verification of AC Policies
e.g., NIST SP 800-192*

Use-based Usage Control (UseCON)

Definitions

• Entities

\[ E \triangleq S \cup O \cup A \]

• Attributes function

\[ att_i: X \mapsto RangeAtt_i \]

• Entity specification

\[ e_i \triangleq [id(e_i) = k, att_1(e_i) = l_1, \ldots, att_n(e_i) = l_n] \]

\[ \forall e_i, e_j \in E: id(e_i) = id(e_j) \iff e_i = e_j \]
Definitions – Use

• A use $u$ represents a record

$$u \triangleq [sid(u) = s. id, oid(u) = o. id, aid(u) = a. id, st(u) = state, att_1(u) = v_1, \ldots, att_n(u) = v_n]$$
Decision making

• Policies
  \[ Policy\_Rule(s, o, a, S, O, A) \triangleq \text{expression}(e_1, \ldots, e_n) \]
  e.g., \( p = p_1 \land p_2 \ldots \land p_n \)

• Type of policies
  • Direct:
    \[ e_i \in \{s, o, a\} \text{ or } e_i \triangleq l \]
  • Indirect:
    \[ e_i \triangleq \text{CHOOSE } x \in E: \text{select}(x, s, o, a, l) \]
  • Complex indirect:
    \[ e_i \triangleq \text{aggregation}([e \in E: \text{select}(e)]) \]
Transition system – Pre model

\[ \text{Init} \triangleq U = \{\} \]

\[ \text{Next} \triangleq \text{Request} \lor \text{preEvaluate} \lor \text{Complete} \]
Transition system – Pre model - Actions

Request ≡ ∃u ∈ (S × A × O):
(∀x ∈ U: (x.sid ≠ u[1].id ∨ x.aid ≠ u[2].id ∨ x.oid ≠ u[3].id)
∧ U' = U ∪ {createUse(u)})

CreateUse(x)
≡ [sid(x) = x[1].id, aid(x) = x[2].id, oid(x) = x[3].id,]
   state(x) = “requested”, att(x) = k
Transition system – Pre model – Actions (continued)

\[ \text{preEvaluate} \triangleq \exists u \in U: \]
\[ \land u.\text{state} = \text{“requested”} \]
\[ \land \text{IF(PolicyRule)} \]
\[ \text{THEN} \]
\[ U' = (\{U \setminus \{u\}\} \cup \{\text{preUpdate}(u)\}) \]
\[ \text{ELSE} \]
\[ U' = (\{U \setminus \{u\}\} \cup \{\text{denUpdate}(u)\}) \]

\[ \text{preUpdate} \triangleq [u \EXCEPT !.\text{st} = \text{“activated”}] \]

\[ \text{denUpdate} \triangleq [u \EXCEPT !.\text{st} = \text{“denied”}] \]
Transition system – Pre model – Actions (continued)

\[ \text{Complete} \triangleq \exists u \in U: \]
\[ \quad \land u.\text{state} = \text{“activated”} \]
\[ \quad \land U' = (U\setminus\{u\}) \cup \{\text{comUpdate}(u)\} \]

\[ \text{comUpdate} \triangleq [u \text{ EXCEPT } !.st = \text{“completed”} ] \]
Transition system – Ongoing model

\[ \text{Init} \triangleq U = \{ \} \]

\[ \text{Next} \triangleq \text{Request} \lor \text{Activate} \lor \text{onEvaluate} \lor \text{Complete} \]
Transition system – Ongoing model - Actions

\[ Activate \triangleq \exists u \in U: \]
\[ \land u.\text{state} = \text{“requested”} \]
\[ \land U' = (\{U\setminus\{u\}\}) \cup \{\text{preUpdate}(u)\} \]

\[ onEvaluate \triangleq \exists u \in U: \]
\[ \land u.\text{state} = \text{“activated”} \]
\[ \land IF(\text{PolicyRule}) \]
\[ \text{THEN} \]
\[ U' = (\{U\setminus\{u\}\}) \cup \{\text{onUpdate}(u)\} \]
\[ \text{ELSE} \]
\[ U' = (\{U\setminus\{u\}\}) \cup \{\text{stopUpdate}(u)\} \]
Verification – Type Correctness

- Assigned values originate from a specific set

\[ \text{TypeCorrectness} \triangleq U \subseteq \text{Uses} \]

\[ \text{SubjectIDs} \triangleq \{s.\text{id}: s \in S\} \]

\[ \text{ObjectId}s \triangleq \{o.\text{id}: o \in O\} \]

\[ \text{ActionIDs} \triangleq \{a.\text{id}: a \in A\} \]

\[ \text{USTATE} \triangleq \{\text{requested, activated, denied, stopped, completed}\} \]
Verification – Violation of safety properties

\[ \text{Safety} \triangleq \Box (\exists u \in U : u.st = \text{“completed”} \implies \Box (u.st \neq \text{“requested”})) \]

<table>
<thead>
<tr>
<th></th>
<th>Current state</th>
<th>Faulty state</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pre model</strong> Completed</td>
<td>Completed</td>
<td>Any other state</td>
</tr>
<tr>
<td>Activated</td>
<td>Completed</td>
<td>Any other state</td>
</tr>
<tr>
<td>Denied</td>
<td>Completed</td>
<td>Any other state</td>
</tr>
<tr>
<td><strong>Ongoing model</strong></td>
<td>Completed</td>
<td>Any other state</td>
</tr>
<tr>
<td>Activated</td>
<td>Completed</td>
<td>Any other state</td>
</tr>
<tr>
<td>Stopped</td>
<td>Completed</td>
<td>Any other state</td>
</tr>
</tbody>
</table>
Verification – Violation of liveness properties

\[ \text{Liveness} \triangleq \forall u \in U : u.st = \text{“activated”} \iff u.st = \text{“requested”} \]

<table>
<thead>
<tr>
<th>Pre model</th>
<th>Current state</th>
<th>Future state</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requested</td>
<td>Activated, Denied, Completed</td>
<td></td>
</tr>
<tr>
<td>Activated</td>
<td>Completed</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ongoing model</th>
<th>Current state</th>
<th>Future state</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requested</td>
<td>Activated, Completed, Stopped</td>
<td></td>
</tr>
<tr>
<td>Activated</td>
<td>Completed, Stopped</td>
<td></td>
</tr>
</tbody>
</table>
## Performance evaluation

<table>
<thead>
<tr>
<th>Model</th>
<th>Uses</th>
<th>Diameter</th>
<th>States Found</th>
<th>Distinct States</th>
<th>Deadlock (sec)</th>
<th>Safety &amp; Liveness (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre</td>
<td>2</td>
<td>6</td>
<td>21</td>
<td>12</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>23</td>
<td>277969</td>
<td>16832</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>31</td>
<td>45533665</td>
<td>560128</td>
<td>53</td>
<td>138</td>
</tr>
<tr>
<td>Ongoing</td>
<td>2</td>
<td>7</td>
<td>33</td>
<td>16</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>25</td>
<td>367873</td>
<td>23808</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>37</td>
<td>79112449</td>
<td>1224704</td>
<td>118</td>
<td>241</td>
</tr>
</tbody>
</table>
Discussion

• Specification of UseCON use management functions in TLA+
  • Pre and Ongoing authorisation models

• Formal guarantees for $\leq 12$ uses

• Future directions
  • Verification of ongoing policies
  • Investigate the application of secBIP
Thank you for your attention!