Access Control Models for Virtual Object Communication in Cloud-Enabled IoT

Asma Alshehri and Ravi Sandhu
Institute for Cyber Security &
Department of Computer Science at UTSA

18th IEEE Conference on Information Reuse and Integration (IRI)
San Diego, California
August 4, 2017

nmt366@my.utsa.edu,
ravi.sandhu@utsa.edu

www.ics.utsa.edu
• Develop an initial set of access control models for IoT within a robust framework.
Figure 1. ACO Architecture for Cloud-Enabled IoT

* Develop access control models for VO communication in two layers:
  A - Operational models
  B - Administrative models
OUTLINE

- Background
- Use case within ACO architecture
- Operational access control for VO communication
- Administrative access control for VO communication
- Current and future research
- Conclusion
• Access control models for IoT.
• The publish and subscribe communication paradigm
  * The publish/subscribe paradigm has various implementation, primarily topic-based and content-based.
Figure 2. Sensing speeding cars within ACO Architecture
A. ACL and Capability Based (ACL-Cap) Operational Model
B. ABAC Operational Model

Four Questions:
- Which VOs are allowed to publish or send a subscription request to a topic’s MB?
- Which MBs should VOs publish to or send a subscription request to?
- Which VOs should a topic’s MB forward data to?
- Which MBs should VOs receive data from?
A. ACL and Capability Based (ACL-Cap) Operational Model

- The operational models recognize sets of entities:
  - Virtual objects (VO) and topics (T)
  - A set of rights $R=\{p,s\}$.
  - $F=\{\text{Forward}\}$

![Diagram of the ACL-Cap Model]

Figure 3. The ACL-Cap Model
A. ACL and Capability Based (ACL-Cap) Operational Model

- The authorization rule for publish is expressed as follows.
  \[
  \text{Auth-Publish}(VO,T) \equiv (T,p) \in \text{Cap}(VO) \land (VO, p) \in \text{ACL}(T)
  \]
- The authorization rule for subscribe is expressed as follows.
  \[
  \text{Auth-Subscribe}(VO,T) \equiv (T,s) \in \text{Cap}(VO) \land (VO, s) \in \text{ACL}(T)
  \]
- The authorization rule for forwarding of published data by a topic’s MB to a VO expressed as follows.
  \[
  \text{Auth-Forward}(T, VO) \equiv VO \in \text{Subscribers}(T) \land T \in \text{Subscriptions}(VO)
  \]

Figure 3. The ACL-Cap Model
A. ACL and Capability Based (ACL-Cap) Operational Model

- The authorization rule for publish is expressed as follows.
  
  \[
  \text{Auth-Publish}(VO,T) \equiv (T,p) \in \text{Cap}(VO) \land (VO, p) \in \text{ACL}(T)
  \]

- The authorization rule for subscribe is expressed as follows.
  
  \[
  \text{Auth-Subscribe}(VO,T) \equiv (T,s) \in \text{Cap}(VO) \land (VO, s) \in \text{ACL}(T)
  \]

- The authorization rule for forwarding of published data by a topic’s MB to a VO expressed as follows.
  
  \[
  \text{Auth-Forward}(T, VO) \equiv VO \in \text{Subscribers}(T) \land T \in \text{Subscriptions}(VO)
  \]

<table>
<thead>
<tr>
<th>Table I</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL OF TOPICS</td>
</tr>
<tr>
<td>$T_1$</td>
</tr>
<tr>
<td>$VS_1$, $p$</td>
</tr>
<tr>
<td>$VS_2$, $s$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table II</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAPABILITY LIST OF VOS</td>
</tr>
<tr>
<td>$VS_1$</td>
</tr>
<tr>
<td>$T_1$, $p$</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
B. ABAC Operational Model

- The operational models recognize sets of entities:
  - Virtual objects (VO) and topics (T)
  - A set of rights $R=\{p,s\}$ and $F=\{\text{Forward}\}$, as before
  - Sets of attributes, virtual object attributes (VOA) and topic attributes (TA), as follows.

  \[
  \text{VOA} = \{\text{VO-Publish, VO-Subscribe, VO-Subscriptions, VO-Location}\} \\
  \text{TA} = \{\text{T-Publish, T-Subscribe, T-Subscribers, T-Location}\}
  \]

![ABAC Operational Model Diagram]

Figure 4. ABAC Operational Model
B. ABAC Operational Model

- The authorization rule for publish is expressed as follows.
  \[ \text{Auth-Publish}(\text{VO}, T) \equiv T \in \text{VO-Publish}(\text{VO}) \land \text{VO} \in \text{T-Publish}(T) \]

- The authorization rule for subscribe is expressed as follows.
  \[ \text{Auth-Subscribe}(\text{VO}, T) \equiv T \in \text{VO-Subscribe}(\text{VO}) \land \text{VO} \in \text{T-Subscribe}(T) \]

- The authorization rule for forwarding of published data by a topic’s MB to a VO expressed as follows.
  \[ \text{Auth-Forward}(T, \text{VO}) \equiv T \in \text{Subscriptions}(\text{VO}) \land \text{VO} \in \text{Subscribers}(T) \]

- We can conjunctively add the following condition to each of the three equations above.
  \[ \text{T-Location}(T) \approx \text{VO-Location}(\text{VO}) \]
• Admins mean users who are authorized to control VO communication, by adjusting configuration of the operational model.
   A. Administrative ACL Model
   B. Administrative RBAC Model
   C. Administrative ABAC Model

• For the ACL-Cap operational model:
  • Who is allowed to add or delete (VO,p) or (VO,s) from ACL of T?
  • Who is allowed to add or delete (T,p) or (T,s) from Capability list of VO?

• For the ABAC operational model:
  • Who is allowed to assign or delete values to/from attributes of T?
  • Who is allowed to assign or delete values to/from attributes of VO?
A. Administrative ACL Model

- The administrative ACL model introduces a set of admin users (A) and admin permissions (AP) as follows.
  \[ A = \{U_1, \ldots, U_{m-1}, U_m\} \]
  \[ AP = \{Own, Control\} \]

Figure 5. Administrative ACL
The authorization rule for admin user U to control T or VO as follow.

\[ \text{Auth-Control}(U,T) \equiv (U,ap) \in ACL(T) \]

\[ \text{Auth-Control}(U,VO) \equiv (U,ap) \in ACL(VO) \]

AP = \{Own, Control\}

Figure 5. Administrative ACL
B. Administrative RBAC Model

- Additionally, RBAC introduces set of administrative roles (AR) and admin permissions (AP) as follows.

\[
AR = \{AR1, ..., ARs\}, \\
AP = (VO \times AP) \cup (T \times AP)
\]

Figure 6. Administrative RBAC
C. Administrative ABAC Model

- Additionally, ABAC introduces administrative attributes for topics (TAA), VOs (VOAA), and users (UAA), as follows.

  TAA = \{T\-Location, T\-Department\}

  VOAA = \{VO\-Type, VO\-Location, VO\-Department\}

  UAA = \{U\-Type, U\-Location, U\-Department\}

Figure 9. Administrative ABAC
C. Administrative ABAC Model

The authorization to use the Control permission with respect to virtual objects or topics is specified as follows.

\[
\text{Auth-Control}(U, VO) \equiv \\
(U\text{-Type}(U) = \text{Own} \lor U\text{-Type}(U) = \text{Control}) \land \\
U\text{-Department}(U) = VO\text{-Department}(VO) \land \\
(VO\text{-type} = \text{sensor} \lor VO\text{-type} = \text{camera}) \land \\
U\text{-location} \approx VO\text{-Location}(VO)
\]

\[
\text{Auth-Control}(U, T) \equiv \\
(U\text{-Type}(U) = \text{Own} \lor U\text{-Type}(U) = \text{Control}) \land \\
U\text{-Department}(U) = T\text{-Department}(T) \land \\
U\text{-location} = T\text{-Location}(T)
\]
CURRENT AND FUTURE RESEARCH

- Current Research:
  - Studying VO communication within AWS IoT.
  - Studying the access control model of VO communication within AWS IoT

- Future research:
  - Proposing access control models for User and Virtual Object communication.
  - Proposing access control models for data accumulated within Virtual objects and cloud services.
* Develop access control models for VO communication in two layers:

A - Operational models
   - ACL and Capability Based (ACL-Cap) Operational Model
   - ABAC Operational Model

B - Administrative models
   - Administrative ACL Model
   - Administrative RBAC Model
   - Administrative ABAC Model
Thanks!