Dynamic Groups and Attribute-Based Access Control for Next-Generation Smart Cars

Maanak Gupta, James Benson, Farhan Patwa and Ravi Sandhu
Institute for Cyber Security,
Center for Security and Privacy Enhances Cloud Computing,
The University of Texas at San Antonio

9th ACM Conference on Data and Application Security and Privacy (CODASPY)
March 25-27, 2019. Dallas, TX, USA

gmaanakg@yahoo.com
http://sites.google.com/view/maanakgupta
Smart Cars Ecosystem

Safety and Assistance

Information and Entertainment

High Mobility, Location Centric
Time Sensitive, Dynamic Pairing
Multiple Fog/Cloud Infrastructures
No More Isolated.

100 million lines of code

Software Reliance, Broad Attack Surface, Untrusted Entities
**Attribute Based Access Control**

- **ABAC**: Decision based on the attributes of entities
- Attributes are name value pair: age (Alice) → 29
- Core entities in ABAC include:
  - Users
  - Objects
  - Environment or Context
  - Operations

**Authorization Policies**: determine rights just in time
- retrieve attributes of relevant entities in request
- Enhance flexibility and fine grained access control
Access Control Needs in Smart Cars

- On-Board Data, Applications and Sensors
- User Privacy Preferences
- Over the Air updates
- V2X fake messages
- Third Party devices
- Loss of Information in Cloud
- Location and time sensitivity of the services.
- In-vehicle communication
Scope of Contribution

➢ Contribution
  ❖ Propose formalized ABAC model for cloud assisted applications.
  ❖ Dynamic groups and user preferences.
  ❖ Implementation of the model in AWS.

➢ Scope
  ❖ Single Central Cloud
  ❖ No direct access and physical tampering
  ❖ Communication Channel is encrypted.
  ❖ Data in Cloud is secure
  ❖ In-vehicle security not considered
Location Groups

- Categorizing wide locations into smaller groups.
- Vehicles dynamically become member based on current GPS, vehicle-type or individual user preferences.
- Ensure relevance of alerts and notifications
Attributes and Alerts

Vehicle moves and are assigned to different groups and inherits their attributes/alerts.

- Speed Limit: 50 mph
- Deer Threat: ON
- Ice on Road: NO

- Speed Limit: 30 mph
- Flood Warning: ON
- Road Work: ON

- Speed Limit: 20 mph
- School Zone: ON
- Amber Alert: ABC123

© Maanak Gupta

World Leading Research with Real World Impact!
Using Location Groups

Administrative Questions:
• How the attributes or alerts of groups are updated?
• How are moving entities assigned to groups?
• How groups hierarchy is created?

Operational Questions:
• How attributes and groups are used to provide security?
• How user privacy preferences are considered?

Reported MQTT message

{"state": {"reported": {"Latitude": "29.4769353", "Longitude": "-98.5018237"}}}
CV-ABAC$^G$ Model
user, sensor, car, mechanic, restaurant

{ location, size, IP, direction, speed, VIN, cuisine-type}
Model Components

{ read, write, control, notify, administrative actions }
Model Components

Cars, traffic lights, smart-devices

Sensor, ECU, on-board apps

Location groups, service-specific, vehicle-type
Model Components

Operational and Administrative Activities
{notification, alerts, group hierarchy updates}
Formal Specification

Basic Sets and Functions
- $S, CO, O, G, OP$ are finite sets of sources, clustered objects, objects, groups and operations respectively [blue circles in Figure 4].
- $A$ is a finite set of activities which can be performed in system.
- $ATT$ is a finite set of attributes associated with $S, CO, O, G$ and system-wide.
- For each attribute $att$ in $ATT$, $Range(att)$ is a finite set of atomic values.
- $attType$: $ATT = \{\text{set, atomic}\}$, defines attributes to be set or atomic valued.
- Each attribute $att$ in $ATT$ maps entities in $S, CO, O, G$ to attribute values. Formally,
  $$att : S \cup CO \cup O \cup G \cup \{\text{system-wide}\} \rightarrow \begin{cases} Range(att) \cup \{\bot\} & \text{if}\ attType(att) = \text{atomic} \\ 2^{Range(att)} & \text{if}\ attType(att) = \text{set} \end{cases}$$
- $POL$ is a finite set of authorization policies associated with individual $S, CO, O, G$.
- $directG : CO \rightarrow G$, mapping each clustered object to a system group, equivalently $CGA \subseteq CO \times G$.
- $parentCO : O \rightarrow CO$, mapping each object to a clustered object, equivalently $OCA \subseteq O \times CO$.
- $GH \subseteq G \times G$, a partial order relation $\geq_g$ on $G$. Equivalently, $parentG : G \rightarrow 2^G$, mapping group to a set of parent groups in hierarchy.
Effective Attributes of Groups, Clustered Objects and Objects (Derived Functions)
- For each attribute att in ATT such that attType(att) = set:
  - $\text{effG}_\text{att} : G \rightarrow 2^{\text{Range}(\text{att})}$, defined as $\text{effG}_\text{att}(g_i) = \text{att}(g_i) \cup \bigcup_{g \in \{g | g_i \geq_g g\}} \text{effG}_\text{att}(g)$.
  - $\text{effCO}_\text{att} : CO \rightarrow 2^{\text{Range}(\text{att})}$, defined as $\text{effCO}_\text{att}(co) = \text{att}(co) \cup \text{effG}_\text{att}(\text{directG}(co))$.
  - $\text{effO}_\text{att} : O \rightarrow 2^{\text{Range}(\text{att})}$, defined as $\text{effO}_\text{att}(o) = \text{att}(o) \cup \text{effCO}_\text{att}(\text{parentCO}(o))$.
- For each attribute att in ATT such that attType(att) = atomic:
  - $\text{effG}_\text{att} : G \rightarrow \text{Range}(\text{att}) \cup \{\bot\}$, defined as $\text{effG}_\text{att}(g_i) = \begin{cases} \text{att}(g_i) & \text{if } \forall g' \in \text{parentG}(g_i). \text{effG}_\text{att}(g') = \bot \\ \text{effG}_\text{att}(g') & \text{if } \exists \text{parentG}(g_i). \text{effG}_\text{att}(\text{parentG}(g_i)) \neq \bot \text{ then select parent } g' \text{ with } \text{effG}_\text{att}(g') \neq \bot \text{ updated most recently.} \end{cases}$
  - $\text{effCO}_\text{att} : CO \rightarrow \text{Range}(\text{att}) \cup \{\bot\}$, defined as $\text{effCO}_\text{att}(co) = \begin{cases} \text{att}(co) & \text{if } \text{effG}_\text{att}(\text{directG}(co)) = \bot \\ \text{effG}_\text{att}(\text{directG}(co)) & \text{otherwise} \end{cases}$
  - $\text{effO}_\text{att} : O \rightarrow \text{Range}(\text{att}) \cup \{\bot\}$, defined as $\text{effO}_\text{att}(o) = \begin{cases} \text{att}(o) & \text{if } \text{effCO}_\text{att}(\text{parentCO}(o)) = \bot \\ \text{effCO}_\text{att}(\text{parentCO}(o)) & \text{otherwise} \end{cases}$

Attributes more Dynamic
Attributes Inheritance
Administrators in the police department can send alert to location-groups in city limits.

\[ \text{Auth}_{	ext{alert}}(u:U, g:G) :: \text{dept}(u) \text{ Police} \land \text{parent-city}(g) = \text{Austin} \land \text{Austin} \in \text{jursidiction}(u). \]

Only mechanic in the technician department from Toyota-X dealership must be able to read sensor in Camry LE. Further, this operation must be done between time 9 am to 6 pm.

\[ \text{Auth}_{\text{read}}(u:U, co:CO) :: \text{role}(u) \text{ Technician} \land \text{employer}(u) = \text{Toyota-X} \land \text{make}(co) = \text{Toyota} \land \text{model}(co) = \text{Camry LE} \land \text{operation}_{\text{time}}(u) \in \{9am,10,11...6pm\} \]
Activity Authorization Decision

Authorization Decision
- A source $s \in S$ is allowed to perform an activity $a \in A$, stated as $\text{Authorization}(a : A, s : S)$, if the required policies needed to allow the activity are included and evaluated to make final decision. These multi-layer policies must be evaluated for individual operations ($\text{op}_i \in \text{OP}$) to be performed by source $s \in S$ on relevant objects ($x_i \in \text{CO} \cup \text{LO} \cup \text{G}$).

Formally, $\text{Authorization}(a : A, s : S) \Rightarrow \text{Auth}_{\text{op}_1}(s : S, x_1), \text{Auth}_{\text{op}_2}(s : S, x_2), \ldots, \text{Auth}_{\text{op}_n}(s : S, x_n)$

Evaluate all relevant policies to make a decision

A restaurant in group A must be allowed to send notifications to all vehicles in location group A and group B.

I only want notifications from Cheesecake factory.
Implementation in Amazon Web Services (AWS)
Vehicles and Groups

4 Location Groups
(static demarcation)

Vehicles movement
(coordinates generated using Google API)

('Received new coordinates from:', 'Vehicle-1')
Sun May 27 02:56:30 2018
Location A
  Car-A : [u'Vehicle-1', u'Vehicle-2']
  Bus-A : []
Location B
  Car-B : []
  Bus-B : [u'Vehicle-6']
Location C
  Car-C : [u'Vehicle-3', u'Vehicle-4']
  Bus-C : []
Location D
  Car-D : []
  Bus-D : [u'Vehicle-5']

Snapshot (table keeps changing)
Implemented Policies

➢ Administrative Policy
  ❖ Road side motion sensor with [id = 1] and current GPS in group [Location-A] can only [modify] attribute [Deer Threat] to value [ON, OFF] for group [Location-A].

➢ Operational Policy
  
  Restaurant Notification Use Case
  System Defined Policy
  ❖ A restaurant located within group [Location-A] can only [send notifications] to members of groups [Location-A, Location-B].
  User Preferences
  ❖ Send notifications only between [7 pm to 9 pm] only on [Wednesdays].
### Performance Metrics

#### Policy Enforcement Time

<table>
<thead>
<tr>
<th>Number of Requests</th>
<th>Policy Enforcer Execution Time (in ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0.0501</td>
</tr>
<tr>
<td>20</td>
<td>0.1011</td>
</tr>
<tr>
<td>30</td>
<td>0.1264</td>
</tr>
<tr>
<td>40</td>
<td>0.1630</td>
</tr>
<tr>
<td>50</td>
<td>0.1999</td>
</tr>
</tbody>
</table>

#### Relevance of Alerts and Notifications

<table>
<thead>
<tr>
<th>n\textsuperscript{th} Request</th>
<th>With ABAC Policy</th>
<th>Without Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>41\textsuperscript{st}</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>42\textsuperscript{nd}</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>43\textsuperscript{rd}</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>44\textsuperscript{th}</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>45\textsuperscript{th}</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>46\textsuperscript{th}</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>
Performance Metrics

Comparing Policy vs No Policy Execution Time
Proposed an **Attribute Based Access Control** solution for cloud assisted Smart Cars.

- Introduced Dynamic Groups
- Supports User Privacy Preferences and Location Centric
- Proof of Concept implementation in AWS

**Future Research**

- Extensive and detailed evaluation
- V2V and V2I secure trusted communication using Edge
- Location preserving approaches
Thank You..!!

Questions, Comments or Concerns

gmaanakg@yahoo.com

https://sites.google.com/view/maanakgupta