Secure Cloud Assisted Smart Cars

Maanak Gupta
Assistant Professor
Department of Computer Science
Tennessee Technological University

CAE Forum

November 13, 2019

mgupta@tntech.edu
www.maanakgupta.com
Cyber Security Landscape

Objectives

Enforce

Enable

POLICY

ATTACKS

What?

Why?

Respond

Defend

Mechanisms

How?

Complement

PROTECT

DETECT

Reference: www.profsandhu.com

© Maanak Gupta
Cyber Security Landscape

Objectives
- Enforce
- Enable

Mechanisms
- Access Control
- Protect
- Detect

POLICY
What?
Why?
How?

ATTACKS

Reference: www.profsandhu.com

© Maanak Gupta
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
The Perfect World.

I TRUST my users.
Everything is Secure. !!

Confidentiality
Integrity
Availability
A user [U] is allowed to perform an operation [OP] on an object [OB] if security policy [P] is satisfied.
A user [U] is allowed to perform an operation [OP] on an object [OB] if security policy [P] is satisfied.
Three Dominant Models: DAC, MAC and RBAC.

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

NIST Guidelines to ABAC
Extended Access Control Oriented Architecture

E-ACO architecture

Vehicular IoT components in architecture
Vehicle moves and are assigned to different groups and inherits their attributes/alerts.
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:

```json
{"state":{"reported":{"Latitude": "29.4769353", "Longitude": "-98.5018237"}}}
```
CV-ABAC\(_G\) Model
Model Components

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}

System Level

System Wide Policies

Individualized Privacy Policies
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 = {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,
  \[
  att : S \cup CO \cup O \cup G \cup \text{[system-wide]} \rightarrow \begin{cases} 
  \text{Range(att) } \cup \{1\} & \text{if } \text{attType(att)} = \text{atomic} \\
  2^{\text{Range(att)}} & \text{if } \text{attType(att)} = \text{set}
  \end{cases}
  \]
- POL is a finite set of authorization policies associated with individual S, CO, O, G.
- directG : CO → G, mapping each clustered object to a system group, equivalently CGA ⊆ CO × G.
- parentCO : O → CO, mapping each object to a clustered object, equivalently OCA ⊆ O × CO.
- GH ⊆ G × G, a partial order relation ≥_g on G. Equivalently, parentG : G → 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 $\text{effG}_{\text{att}}(g_i) = \text{att}(g_i) \cup \bigcup_{g \in \{g_i | g_i \geq_g g_j\}} \text{effG}_{\text{att}}(g)$.
  - $\text{effCO}_{\text{att}} : CO \rightarrow 2^{\text{Range}(\text{att})}$, 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:
  - $\text{effG}_{\text{att}} : G \rightarrow \text{Range}(\text{att}) \cup \{\perp\}$, defined as $\text{effG}_{\text{att}}(g_i) = \begin{cases} \text{att}(g_i) & \text{if } \forall g' \in \text{parentG}(g_i). \text{effG}_{\text{att}}(g') = \perp \\ \text{effG}_{\text{att}}(g') & \text{if } \exists \text{parentG}(g_i). \text{effG}_{\text{att}}(\text{parentG}(g_i)) \neq \perp \text{ then select parent } g' \text{ with } \text{effG}_{\text{att}}(g') \neq \perp \text{ updated most recently.} \end{cases}$
  - $\text{effCO}_{\text{att}} : CO \rightarrow \text{Range}(\text{att}) \cup \{\perp\}$, defined as $\text{effCO}_{\text{att}}(co) = \begin{cases} \text{att}(co) & \text{if } \text{effG}_{\text{att}}(\text{directG}(co)) = \perp \\ \text{effG}_{\text{att}}(\text{directG}(co)) & \text{otherwise} \end{cases}$
  - $\text{effO}_{\text{att}} : O \rightarrow \text{Range}(\text{att}) \cup \{\perp\}$, defined as $\text{effO}_{\text{att}}(o) = \begin{cases} \text{att}(o) & \text{if } \text{effCO}_{\text{att}}(\text{parentCO}(o)) = \perp \\ \text{effCO}_{\text{att}}(\text{parentCO}(o)) & \text{otherwise} \end{cases}$
Administrators in the police department can send alert to location-groups in city limits.

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

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.

\[ \text{Auth}_{\text{read}}(u:U, co:CO) :: \text{role}(u) \; \text{Technician} \land \text{employer}(u) = \text{Toyota-X} \land \text{make}(co) = \text{Toyota} \land \text{model}(co) = \text{Camry LE} \land \text{operation\_time}(u) \in \{9am,10,11...6pm\} \]
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 ($op_i \in OP$) to be performed by source $s \in S$ on relevant objects ($x_i \in CO \cup O \cup G$).

Formally, $\text{Authorization}(a : A, s : S) \Rightarrow \text{Auth}_{op_1}(s : S, x_1), \text{Auth}_{op_2}(s : S, x_2), \ldots, \text{Auth}_{op_n}(s : S, x_3)$

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.

System defined

DECISION

User Preference

© Maanak Gupta
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)
Performance Metrics

![Bar Chart](chart.png)

- **Cars-Notified (Deer Threat)**
- **Cars-Notified (Car Pool)**
- **Cars Notified (Without Policy)**

<table>
<thead>
<tr>
<th>Random n&lt;sup&gt;th&lt;/sup&gt; Action Requests</th>
<th>Number of Cars</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>15, 5</td>
</tr>
<tr>
<td>13</td>
<td>20, 33</td>
</tr>
<tr>
<td>25</td>
<td>6, 23</td>
</tr>
<tr>
<td>37</td>
<td>18, 10</td>
</tr>
<tr>
<td>46</td>
<td>33, 17</td>
</tr>
</tbody>
</table>
Performance Metrics
Let’s Talk ..!!

Questions, Comments or Concerns

mgupta@tntech.edu

www.maanakgupta.com