Securing Next Generation Smart Cars: Access Control Needs and Solutions

Maanak Gupta
PhD Student
Advisor: Ravi Sandhu

Institute for Cyber Security,
Center for Security and Privacy Enhanced Cloud Computing,
Department of Computer Science
University of Texas at San Antonio

ICS C-SPECC Student Seminar
June 11, 2018
Smart Cars Ecosystem

Cloud to Cloud

DMV

Fog to Fog

Vehicular Cloud

Internet Cloud

Mechanic

© Maanak Gupta

World Leading Research with Real World Impact!
➢ On-Board Application and Sensors
  • Tesla and Jeep X
➢ Over the Air updates
➢ V2X fake messages
➢ In-vehicle ECU communication
➢ Personal Data
➢ Third Party devices
➢ User Privacy Preferences
➢ Spoofing, Ransomware, Injection...
➢ Loss of Information in Cloud
Security and Privacy Requirements

➢ On-Board Application and Sensors
  • Tesla and Jeep X
➢ Over the Air updates
➢ V2X fake messages
➢ In-vehicle ECU communication
➢ Personal Data
➢ Third Party devices
➢ User Privacy Preferences
➢ Spoofing, Ransomware, Injection...
➢ Loss of Information in Cloud

- Software Reliance
- Broad Attack Surface
- Untrusted Entities
Extended Access Control Oriented Architecture

a) Extended ACO Architecture for Connected Car and IoV

b) Connected Car and Vehicular IoT Components in Extended ACO Layers
Authorization Framework

Cloud Services Level
- AP - AP
- FG - CL
- CSR - CSR
- AP - CSR
- FG - FG
- CL - CL

Virtual Object Level
- VCO - VOB
- AP - VOB
- AP - CL-VOB - OB
- AP - CL-VCO - CO
- VOB - VOB
- OAP - VOB
- OAP - VOB
- OAP - OB
- OB - VOB
- OAP - VOB
- CO - VCO

Object Level
- U - OB
- AP - OAP
- AP - OB
- CO - OB
- CO - CO
- U - OAP
- U - OB
- AP - CO

Access Control Strategies

- Static vs Dynamic
- What kind of relationship they have?
  - Owner
  - Manufacturer
  - Friend
- Multi-Layered
- Groups Based
- Trusted Interaction
  - How I trust you?
  - Previous interaction..?
- ABAC, ReBAC Models
- Who will administer?
- Data in Cloud, cross cloud sharing, how?
Dynamic Groups and Attribute Based Access Control
Location Groups
CV-ABAC_G Model

Activity Decision

System Level

POL
ATT

POL
ATT

POL
ATT

POL
ATT

POL
ATT

POL
ATT

One to Many
Many to Many
Zero or More

Attribute / Policy Association
Many to Many Dynamic Group Association
One to Many Association

© Maanak Gupta

World Leading Research with Real World Impact!
('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']
ABAC Policy

```json
{
  "Deer_Threat": {
    "Source": {
      "1": {
        "Location": {
          "Location-A": {
            "Group": ["Location-A"]
          },
          "Location-B": {
            "Group": ["Location-B"]
          }
        }
      }
    }
  },
  "car_pool_notification": {
    "Source": {
      "Location-A": {
        "destination": {
          "Location-A": {
            "Notification": ["Car-A"]
          },
          "Location-B": {
            "Notification": ["Car-A", "Car-B", "Car-C"]
          },
          "Location-C": {
            "Notification": ["Car-C", "Car-D"]
          },
          "Location-D": {
            "Notification": ["Car-A", "Car-C", "Car-D"]
          }
        }
      }
    }
  }
}
```
Performance Metrics

<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>

<table>
<thead>
<tr>
<th>nth Request</th>
<th>Cars Notified With ABAC Policy</th>
<th>Cars Notified Without Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>41st</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>42nd</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>43rd</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>44th</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>45th</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>46th</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>

Graph showing the relationship between the number of action requests and the time taken with and without ABAC policy.