A Novel Fine-grained Access Control System for Multi-user Multi-device Smart Home Systems


FIU Electrical & Computer Engineering

Annual Computer Security Applications Conference (ACSAC) 2019 December 12th, 2019
Problem Scope

Binary access control
Any authorized user can get access to all the smart home devices installed in the system.

Impulsive command execution
Any command given by an authorized user is executed by the system without considering overall demand.

Transitive authorization
A newly added user can add other users in the system with full access privilege without notifying the device owner.

Device usage monitoring
No central monitoring tool is available to track the device usage in a multi-user environment.
Access Control Needs in Smart Home

We performed a user study to understand the need of fine-grained access control system in smart home.

We explored and surveyed user preferences for different multi-user multi-device scenarios.

Our study includes 72 real-life smart home users.

<table>
<thead>
<tr>
<th>Expectation of participants</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need of access control</td>
<td>80.6%</td>
</tr>
<tr>
<td>Need of policy negotiation</td>
<td>71%</td>
</tr>
<tr>
<td>Conflict resolution</td>
<td>72.2%</td>
</tr>
<tr>
<td>Specific restriction</td>
<td>86.1%</td>
</tr>
<tr>
<td>Usage monitoring</td>
<td>75%</td>
</tr>
<tr>
<td>Importance of flexibility</td>
<td>74.3%</td>
</tr>
</tbody>
</table>

We propose **KRATOS**, a multi-user multi-device aware access control system for smart environment.

Multi-user Multi-device-aware Access Control System

- Design of a multi-user multi-device-aware access control system for smart home systems.

Formal Policy Language

- Build a formal policy language to understand the conflicting demands in a multi-user smart home environment.

Automatic Policy Negotiation

- Design an automatic policy negotiation engine to resolve conflicting demands in smart environment.

Implement in Real-life Smart Environment

- Implement proposed access control system in real-life smart environment and evaluate the system with real smart device users.
**KRATOS Architecture**

**Workflow of KRATOS**

- Define Policy
- Gather Policies
- Negotiate Conflicts
- Rule Generation
- Enforcement

**Interfaces of KRATOS**

**User interaction module**

- User Management Module
- Policy Management Module
- Login
- Login
- Login
- Login

**Policy input module**

- Policy Management Module
- Input User Email
- Input User Email
- Input User Email
- Input User Email

**Notification system**

- New alert
- New alert
- New alert
- New alert
- New alert
- New alert
Evaluation

- KRATOS is evaluated with **309 different policy sets including 213 demand conflicts and 24 restriction policies**.
- KRATOS successfully detect **5 different types of access control threats with 100% success rate with minimal overhead**.
- KRATOS introduced on average **289 ms latency** for different variables in the system (number of policies, conflicts, users, and devices).

<table>
<thead>
<tr>
<th>Threat model</th>
<th>No of occurrence s</th>
<th>Success rate</th>
<th>Average detection time (s)</th>
<th>Average notification time(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over privileged</td>
<td>10</td>
<td>100%</td>
<td>0.25</td>
<td>0.4</td>
</tr>
<tr>
<td>Privilege abuse</td>
<td>10</td>
<td>100%</td>
<td>0.4</td>
<td>0.6</td>
</tr>
<tr>
<td>Privilege escalation</td>
<td>10</td>
<td>100%</td>
<td>0.47</td>
<td>0.6</td>
</tr>
<tr>
<td>Unauthorized access</td>
<td>10</td>
<td>100%</td>
<td>0.35</td>
<td>0.52</td>
</tr>
<tr>
<td>Transitive privilege</td>
<td>10</td>
<td>100%</td>
<td>0.28</td>
<td>0.45</td>
</tr>
</tbody>
</table>
Conclusions

• Existing smart home systems do not offer any fine-grained access control system to address complex, asymmetric, and conflicting demands in a multi-user smart home environment.

• We proposed KRATOS, a novel multi-user multi-device-aware access control system for smart home.

• We designed KRATOS as priority-based access control system which assigns priority to each authorized users to resolve conflicting demands and implement selective restriction in device usage for specific users.

• We implemented KRATOS in Samsung SmartThings platform and evaluated with 309 different policy sets where KRATOS achieved high success rate with minimal overhead.
Thank You!

Please feel free to join our poster presentation session for more information!

Name: Amit Kumar Sikder
Email: asikd003@fiu.edu
Personal Website: https://nweb.eng.fiu.edu/asikd003
Lab Website: https://csl.fiu.edu/
Project Link: https://arxiv.org/abs/1911.10186