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

Amit Kumar Sikder, Leonardo Babun, Z. Berkay Celik, Abbas Acar, Hidayet Aksu, Patrick McDaniel, Engin Kirda, and A. Selcuk Uluagac

FIU | Electrical & Computer Engineering

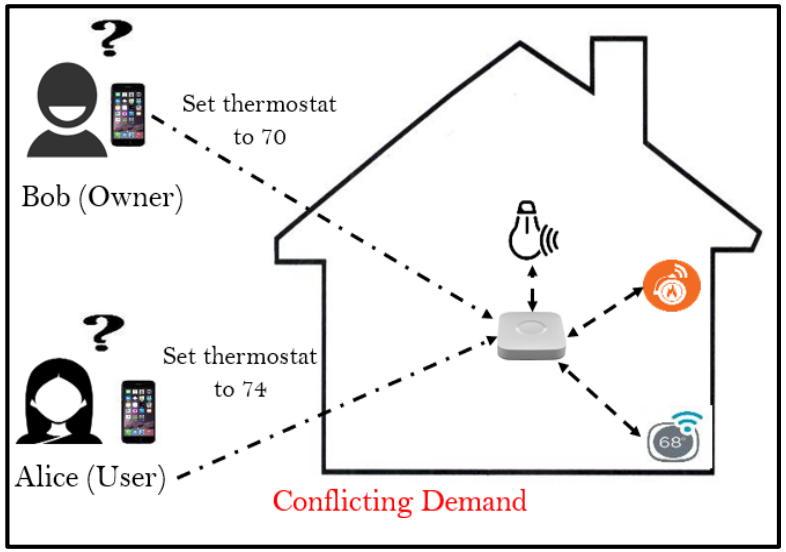
CSL Cyber-Physical Systems Security Lab

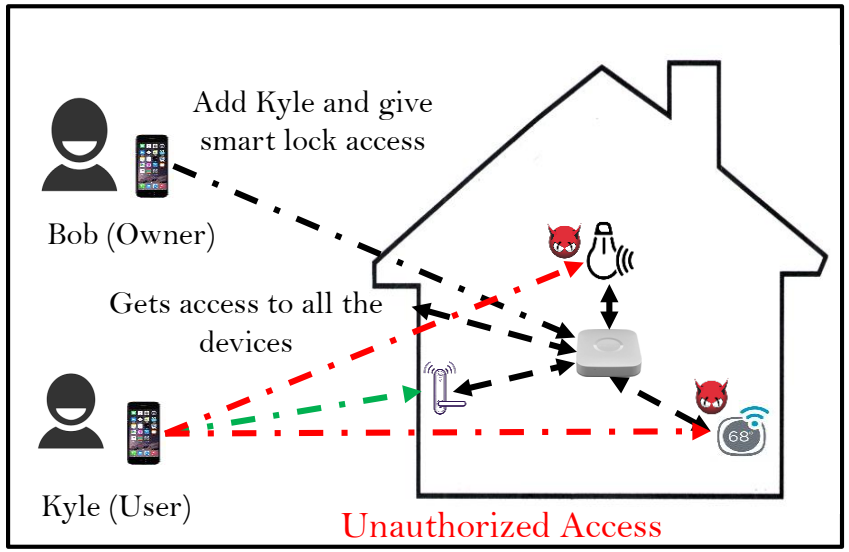
PURDUE UNIVERSITY

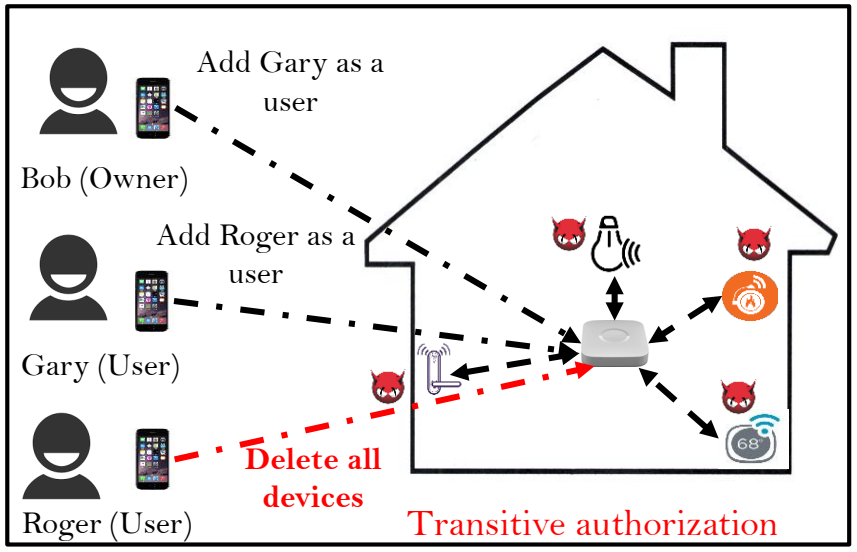
NORTHEASTERN UNIVERSITY BOSTON, MASSACHUSETTS

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 consider 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 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.

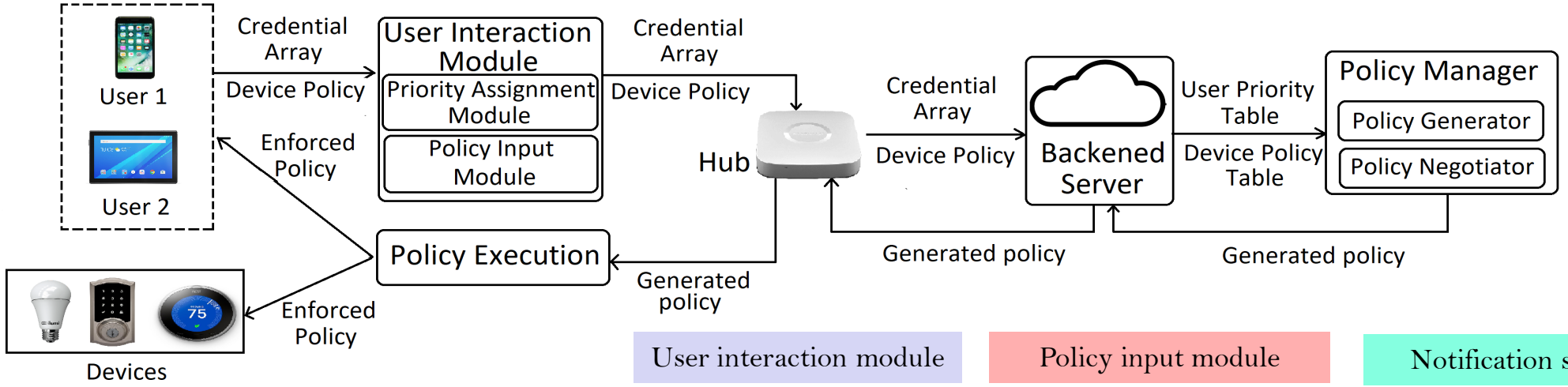
Our study includes 72 real-life smart home users.

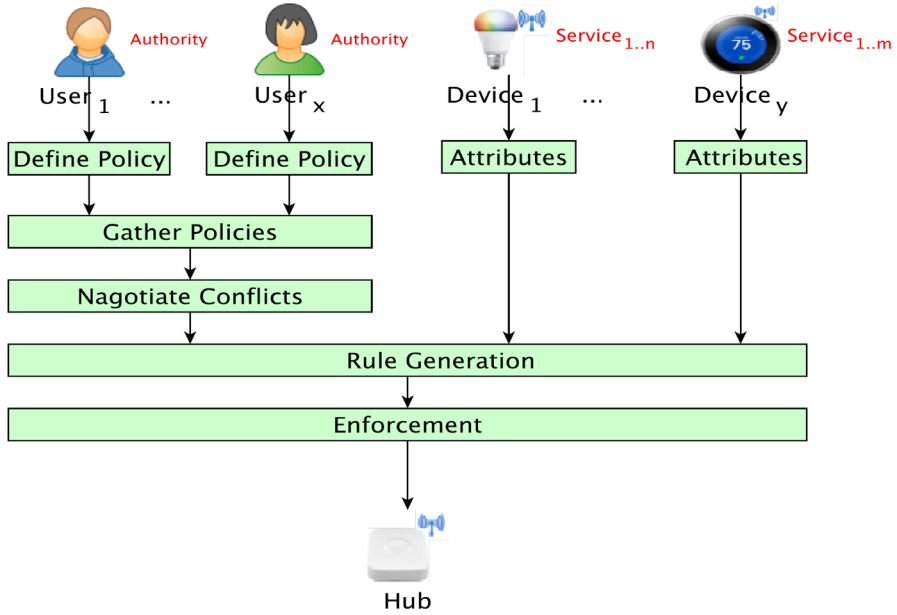
Expectation of participants	Percentage
Need of access control	80.6%
Need of policy negotiation	71%
Conflict resolution	72.2%
Specific restriction	86.1%
Usage monitoring	75%
Importance of flexibility	74.3%

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.

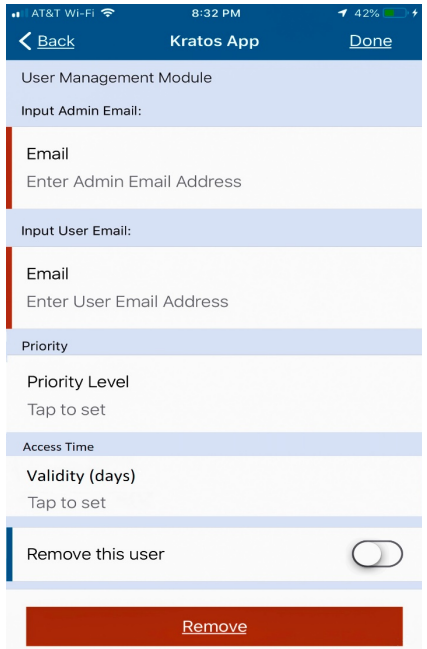
KRATOS Architecture



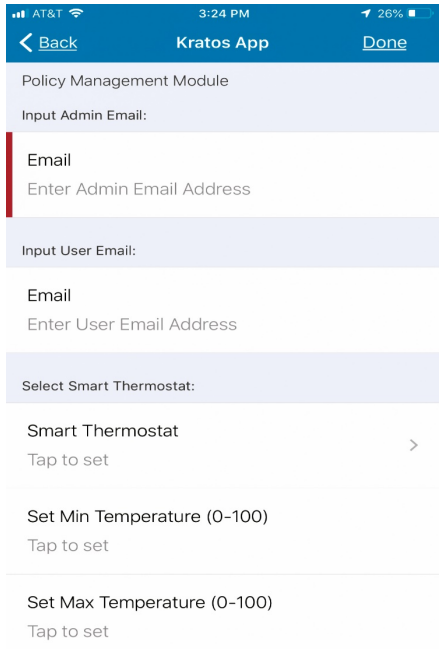


Workflow of KRATOS

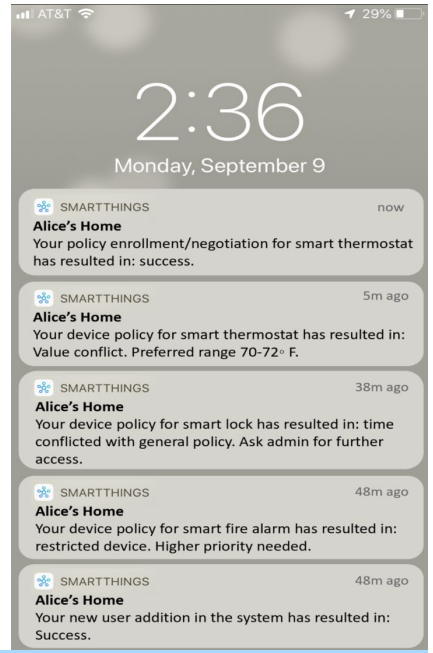
User interaction module



Policy input module



Notification system

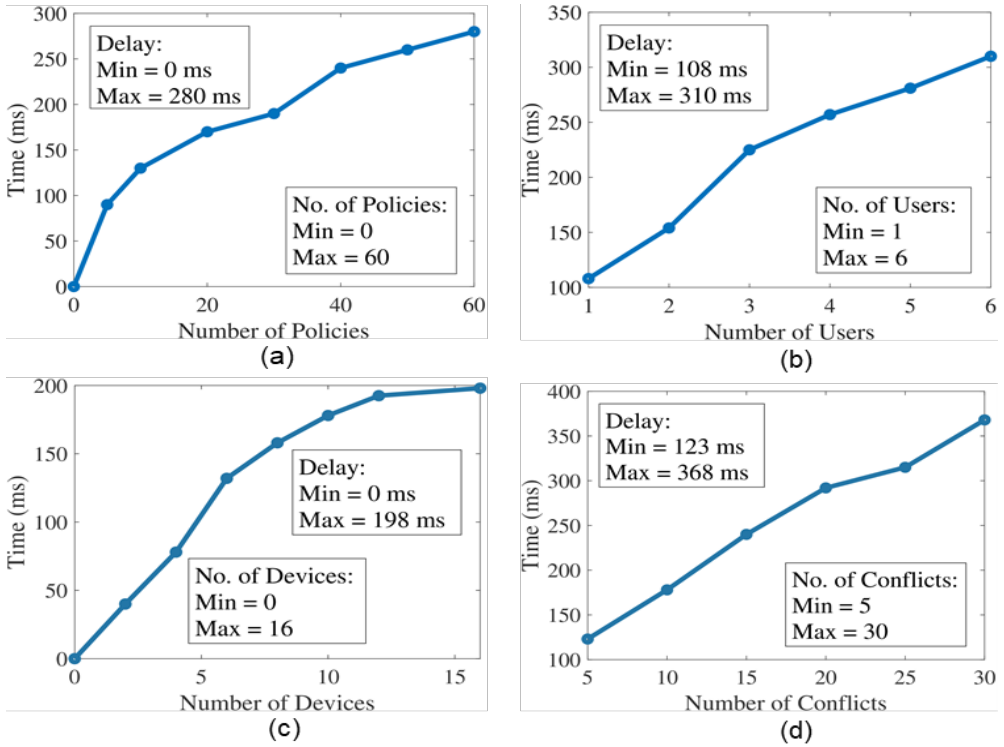


Interfaces of KRATOS

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).

Threat model	No of occurrences	Success rate	Average detection time (s)	Average notification time(s)
Over privileged	10	100%	0.25	0.4
Privilege abuse	10	100%	0.4	0.6
Privilege escalation	10	100%	0.47	0.6
Unauthorized access	10	100%	0.35	0.52
Transitive privilege	10	100%	0.28	0.45



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