



R&D SH W CASE 2021

Technology, Social Impact

A Multi Perspective Access Control in a Smart Home

We aim to design a practical access control system for smart homes that grant fine-grained device privileges to users. We allot privileges based on multiple perspectives (i) the relationship of the user with the device, (ii) the location and risk of the device and (iii) the current environment.

Fine-grained Privileges

Most devices(example: Philips Hue) in the market allow only access to all or none of a device's privileges. They do not let users pick a subset of privileges for any devices' controls. Consider Krish (a child user) wanting to access some smart devices in the Kitchen. Figure 1 shows the granted privileges in an all (or none) privileges scenario.

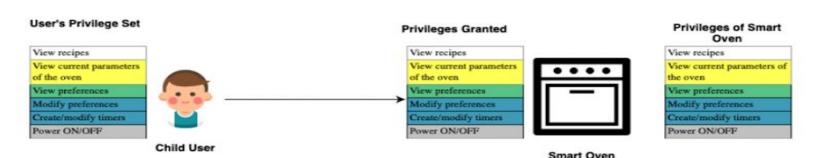


Figure 1:User being allotted all the privileges for an Oven.

Fine grained privilege or privilege is a control that provides access to perform an atomic action or a state of information of a device. Allowing users to allot fine-grain privileges is beneficial from a security standpoint as users can be given only the required privileges of a device[1].

A user role is a subset of privileges of a device, given to a user based on their relationship and eligibility. We propose the following six roles:

- Device Owners (U_1) can access all privileges and settings.
- Normal Users (U₂) can change only software based settings.
- Limited Users (U₃) can access all privileges except settings.
- Home Child User (U_4) can access private information but are restricted to dangerous and sensitive content.
- Adult Guest Users (U₅) can access sensitive content but are restricted to private information
- Guest Child User (U₆) are restricted to both sensitive content and private information.

A user can be assigned any one role for a device. Thus, a child may be given child access privileges U_3 for the TV, but would be given administrative privileges U_1 for the Light in his room. We assume Krish has been given the same child role for all devices in the Kitchen 2 in this example. This first step of user role selection eliminates dangerous privileges being given to the child.



Security Levels

Knowing the criticality of a privilege helps us understand the risks associated with assigning it to a smart home member.

- 1S when misused can cause loss of life, theft and reconnaissance.
- 1P when misused can cause major information and identity loss and reconnaissance.
- 2S when misused can cause an indirect risk of life, mental disturbance, torture.
- 2P when misused can reveal device usage details of daily habits which may be correlated
- 3S when misused can cause monetary loss due to repair and replacement of devices(usually because of overuse).
- 3P when misused can reveal settings of devices, which can pose a threat only if corroborated with the user's personal details.

First level privileges typically cause direct harm to the members of the home. Second level privileges cause indirect, temporary harm/discomfort to the members of the home. Third level privileges cause harm to the devices and property of the users. A user in possession of a large number of critical(lower in rank) security/privacy privileges can pose a big potential risk to the smart home.

Prohibitions

A complete user privilege set of a member of the home would be created by combining all her/his user roles for all devices in the smart home. We provide the facility to restrict certain privileges from the privilege set based on the device's risk-level, location and environment. Environments are socio-temporal constructs (like summers, evenings). Here, Krish is prohibited from using any 1S security level privileges. The updated privilege set after prohibitions is given in Figure 3. Prohibitions add an additional layer of safety to the user and house as he is restricted from 'Changing the temperature' of the Kitchen.

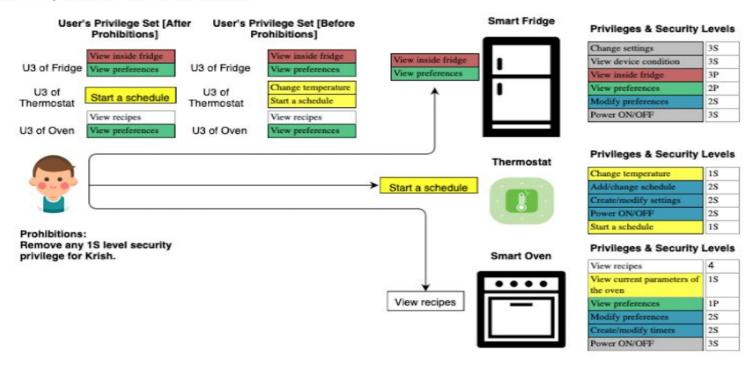


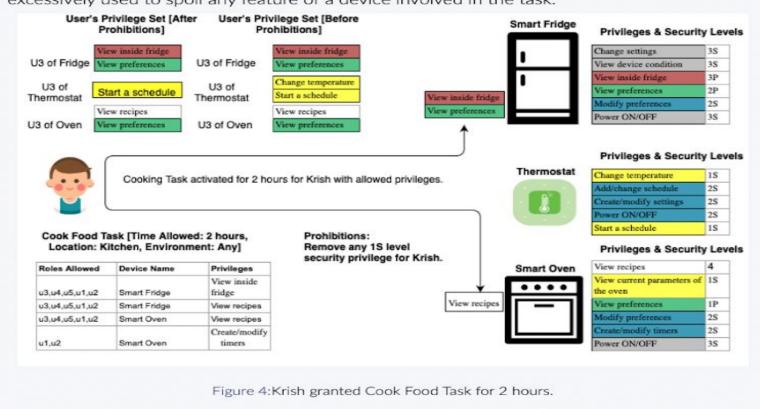
Figure 3:Krish's Privilege set after adding prohibitions.

Tasks

A task[2] is an activity performed by users in a smart home. Tasks are performed by the combined use of the available smart devices in the smart home environment. Thus, certain privileges from each device are needed to execute a task. Tasks can also be created on an ad-hoc basis by extending upon a generic privilege set to provide safe environments to users and devices.

A task is equivalent to session in the RBAC terminology. To maintain static separation of duties, we do not allow two roles for a user in the same session in accordance with NIST-RBAC standard[3]. Task-based systems also ensure grant of privileges for a limited period of time. This acts as a second check to prevent threats due to over-privileges.

Figure 4 shows Krish being given privileges to perform the 'Cook Food' task. The granted privileges disallow Krish to spoil contents of the Fridge or any appliances by forbidding Him to make changes to the Thermostat. The 2-hour time limit for 'Cook Food' ensures no privilege is excessively used to spoil any feature of a device involved in the task.



Summary

We plan to formally define and deploy our model on AWS Greengrass to validate our solution.

References

- [1] Safwa Ameer, James Benson, and Ravi Sandhu. The egrbac model for smart home iot.
- In 2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI), pages 457--462, IEEE, 2020.
- [2] Patrick CK Hung, Kamalakar Karlapalem, and JW Gray. A study of least privilege in capbased-ams.
 - In Proceedings. 3rd IFCIS International Conference on Cooperative Information Systems (Cat. No. 98EX122), pages 208--217. IEEE, 1998
- [3] Ravi Sandhu, David Ferraiolo, Richard Kuhn, et al.
- The nist model for role-based access control: towards a unified standard.