A Multi Perspective Access Control in a Smart Home

Shravya Kanchi
International Institute of Information Technology Hyderabad
shravya.k@research.iiit.ac.in

Kamalakar Karlapalem
International Institute of Information Technology Hyderabad
kamal@iiit.ac.in

ABSTRACT

Existing methods to manage privileges in smart home systems have not considered allocating privileges to users based on (i) the relationship of the user with the device, (ii) the location and risk of the device and (iii) the current environment. In this work, we take a multi perspective view on the problem of sharing fine-grained privileges of IoT devices among multiple users in a smart home. We propose the concepts of user role (subset of privileges specific to each device), tasks and security levels (labels for each privilege) to allot right privileges to users. Thereby, limiting the exploitation of privileges assigned to legitimate insiders of the house. Thus, our work matches the aspirations of previous surveys [8] on building a comprehensive access control system to manage privileges in a shared smart home.

CCS CONCEPTS

• **Security and privacy** → **Access control**; **Usability in security and privacy**.

KEYWORDS

Internet of Things, smart home, over-privilege, multi-user

ACM Reference Format:
Shravya Kanchi and Kamalakar Karlapalem. 2021. A Multi Perspective Access Control in a Smart Home. In *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy (CODASPY '21), April 26–28, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3422337.3450324

1 INTRODUCTION

The smart home environment is a multi-device multi-user environment. Users operate a certain device (need permissions to do so) usually through a smartphone-based Application. Most Applications provide access to control a single IoT device (example: Philips Hue), whereas few Applications allow the control of more than one device (example: Samsung Smartthings). Further, Applications can either provide access to all (or none) of the controls of a device only a few controls. **Fine-grained privilege** or **privilege** is a control that performs an atomic action OR accesses a state of information of a device. Turning UP the volume is an atomic action. Similarly, displaying the battery status is a single data point of information. Allowing users to allot fine-grain privileges is beneficial from a security standpoint as only required privileges of a device[1] can be given. However, not many devices (example: Philips Hue) in the market have adapted their access management systems to grant fine-grained privileges of devices. Moreover, those Applications that do offer the option of fine-grained privileges, often assign more privileges than required, thus, compromising the security and privacy of the house[3].

1.1 Security Issues in a Smart Home

Consider an eight-year-old requesting to control the smart oven in the house. She requests to use the Gas Stove to heat food. Ideally, the Application must prevent usage as it is a risky device for a child (or allow only with the supervision of an adult). Though the same might not be applicable for a teenage user or an adult.
Over-privileging: is when a user has more privileges than what is required by them to perform their tasks.
Under-privileging: is when a user has lesser privileges than what is required by them to perform their tasks.

While over-privileging can cause serious harm to the household due to malicious insiders, under-privileging impedes users to perform their desired activities smoothly.

1.2 Need of Access control

Every home experiences disparate social situations due to its members' varying dynamics, which impacts the usage pattern of the shared smart devices[2]. Users in a smart home should not be given the same role for all device in the home[4]. For example, a child may be given access to a subset of privileges for the TV, but she needs administrative privileges for the Light in her room. Privileges need to be appropriately distributed and shared among the members of the home based on specific social conditions of the home and usage of smart devices.

An improper grant of privileges can lead to a potential loss of money, violation of the family members' privacy, nuisance in the form of noise, heat or light pollution from devices, harm to the value system within the family due to spread of sensitive content. Since devices in the market are still adapting to the concepts of fine-grained privileges, not many systems have been designed to give privileges for a shared device in a multi-user setup. To our knowledge, no previous access control system has assigned role-specific privileges for a device to a user. In this paper, we propose an access control system that allots privileges according to the relationship of a person with the device and weighs in other practical factors like location, environment, and risk level of the device to make this decision. We believe that these factors form the basis of the decision for granting appropriate privileges.

CODASPY '21, April 26–28, 2021, Virtual Event, USA

ACM ISBN 978-1-4503-8143-7/21/04.
https://doi.org/10.1145/3422337.3450324

2 BACKGROUND

A **user role** is a subset of privileges of a device, given to a user based on their relationship and eligibility. Ex: A guest role for a device gets access to only certain non-private functions/privileges. The user roles we proposed are as follows:

Device Owners(U_1): are prime administrators of the device. They can add other users and define the roles of other users for the device. Being a master user of the device, they have full control over the device including **hardware** and **software settings**.

Normal Users(U_2): are second in line to make critical changes to the device. They get control over the **Application-oriented settings** of the device. They only differ from U_1 users in master controls and hardware related capabilities.

Limited Users(U_3): are capable of performing all actions over the devices. They can access all the privileges except the ability to make hardware and software changes to the device.

We assume that users (U_1), (U_2), (U_3) are adult users and are permanent members of the house. Thus, they can view **private** details from the device. Private details include the preferences, history, bank details, and health records of the household's users.

Home Child User(U_4): is a child, which restricts her/him access to the sensitive content (if any) of the device but gives her/him right to view **private** details of the home along with the capabilities given to that of a U_3 user. **Sensitive** content includes information, text, or videos not suitable for the reception of a child. For example, adult and violent content.

Adult Guest Users(U_5): are treated as a temporary (limited) members of the residence who cannot access any private information of the device.

Guest Child User(U_6): is given access to **non-private privileges** of the device along with the access to privileges that are **restrictive towards sensitive content**.

A complete *user privilege set* of a member of the home would be created by combining her/his user roles for all devices in the smart home.

A **task** [5] 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.

We use a task-based approach to grant of privileges to multi-users. 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 following NIST-RBAC standard[7]. Task-based systems also ensure grant of privileges for a limited period. This acts as a second check to prevent threats due to over-privileges. Since the number of privileges sanctioned in a task is limited, it is easier to track the privileges to track malicious insiders.

2.1 Security & Privacy Levels

Knowing the criticality of a privilege helps us understand the risks associated with assigning it to a smart home member. Each privilege is given a security/privacy label based on the proposed hierarchy. If a privilege does not fit in any of the levels, it is assigned a '4' label.

1S - First Level Security Privilege (Personal Level): when misused can cause loss of life, theft and reconnaissance. For example, disarming a security system.

1P - First Level Privacy Privilege (Personal level): when misused can cause major information and identity loss and reconnaissance—for example, viewing credit card details.

2S - Second Level Security Privilege (Indirect Personal Level): when misused can cause an indirect risk of life, mental disturbance, torture—for example, changing the temperature in a thermostat.

2P - Second Level Privacy Privilege (Indirect Personal Level): when misused can reveal device usage details of daily habits which may be correlated with user habits. But these details standalone cannot disclose information about the users of the home. For example, viewing the shopping history of a member.

3S - Third Level Security Privilege (Device Level): when misused can cause monetary loss due to repair and replacement of devices(usually because of overuse). For example, the ability to switch the smart plug on/off.

3P - Third Level Privacy Privilege (Device Level): when misused can reveal settings of devices, which can pose a threat only if corroborated with the personal details of the user. For example, the ability to view the current settings of the shower.

A user in possession of a large number of critical (higher-ranked) security/privacy privileges can cause significant harm to the people and devices of the smart home.

3 MULTI PERSPECTIVE ACCESS CONTROL

To allot least privileges to users in a suitable manner and prevent further exploitation of these privileges by users, we propose the following system. Appropriate privileges of a device are mapped to user roles and marked with appropriate security levels. Every user's privilege set is determined. Attributes are location of a device, risk of a device and environment (socio-temporal constructs like summer, evenings, etc.) of an event. Our model accommodates prohibitions to be defined against these attributes for specific users in their privilege set. This set is then used to determine his/her eligibility perform certain tasks set up by the administrator. Thus, a user gets only indirect access to their privileges through the tasks requested by them.

Figure 1 shows the functioning of our model. Here, Krish (a child user) wants to perform the task of cooking food. For the sake of simplicity, we assume he has been given child roles U_3 for devices Thermostat, Fridge and Oven present in the Kitchen. This first step of user role selection eliminates giving dangerous privileges. Next, Krish is prohibited from using any **1S** privilege. This prohibition from the administrator's side adds an additional layer of safety as he is restricted from 'Changing the temperature' of the Kitchen.

The task disallows Krish to spoil contents of the Fridge by forbidding Him to start any schedule on the Thermostat. On the other hand, it guarantees Krish all the safe privileges needed to cook food as per his eligibility. The arrows show the allowed privileges in Figure 1. The 2-hour limit for 'Cook Food' ensures no privilege is excessively used to spoil any feature of a device involved in the task. For example, in Samsung Fridges, the 'View Inside' feature allows users to watch the items' live stream inside the Fridge. To cause mischief, Krish could continuously turn ON and OFF the

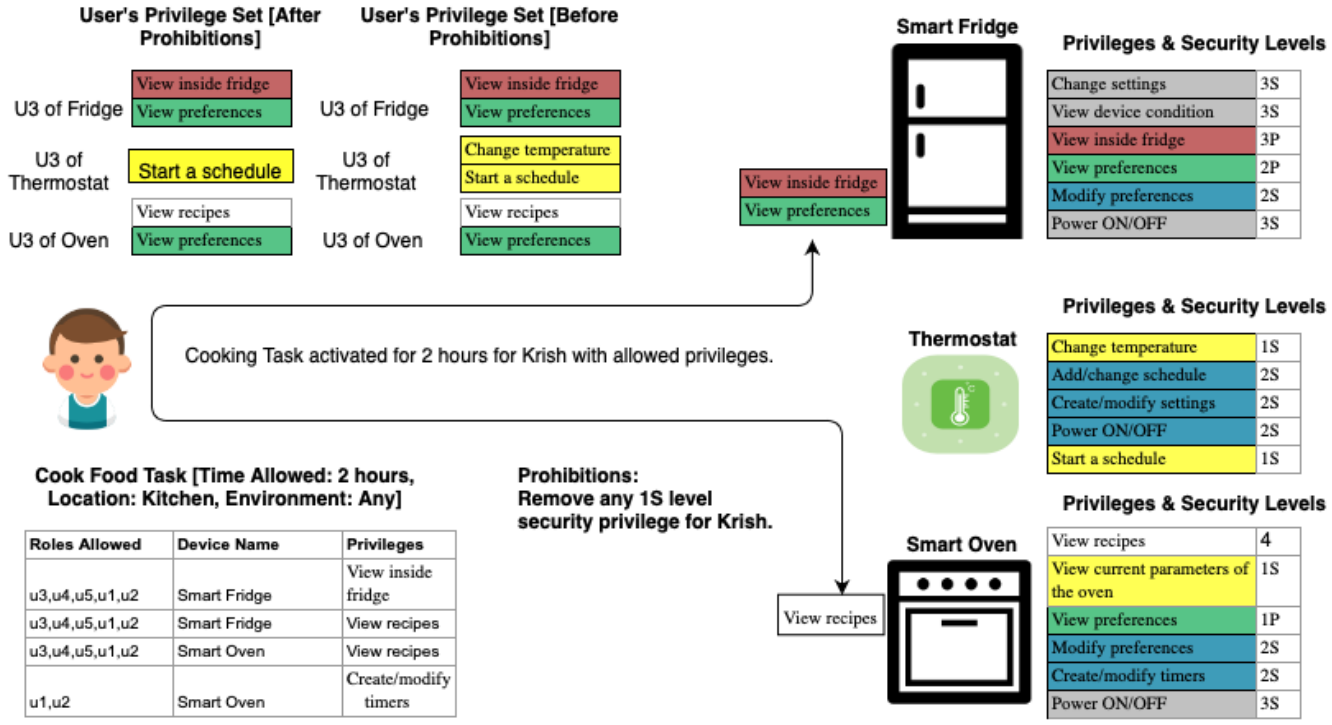

Figure 1: Child User granted Cook Food Task

feed, consequently damaging the camera(assuming he would not be able to cause damage in 2 hours). Note that prohibitions can be customized based on the location, environment and risk level of the device as well for a user. For example, guests can be prohibited to use their U_5 or U_6 privileges for devices in the host's bedrooms.

4 RELATED WORK

Jang, Chabra et. al [6] stated the need to design a multi-user, fine-grained privilege allocation model. They also created different user roles for devices and grouped privileges according to different security levels. Our model has significant differences in utilizing user profiles. Firstly, we propose an extensive list of user roles. Secondly, we do not assume the same user role for all devices in the smart home. Our work is closely related to Ameer's [1] EGBRAC system to grant privileges among users in a home. While we attempt to solve the same problem, our work is superior to theirs in the following aspects:
(a) The roles in our work are selected from a preset list. Thus we lift the burden from the administrator to come up with new roles. Also, every user has been given a different role specific to a device.
(b) Our work allows the prohibition of certain privileges based on multiple perspectives/attributes. Though they provide a facility to make such a configuration in their system, administrators may/not always foresee the need to block vulnerable privileges.
(c) Our model is easy to configure as administrators only have to choose a user role for each device and create tasks. Similarly, for role revocation the admin has to assign just another role for a user.

5 SUMMARY

We have designed a practical model that gives least privileges to users of a smart home according to the user's relationship with the devices considering the time, place and environment of the devices. Our solution relies on a smart home operating system that grants privileges just for a limited time for users to perform tasks. 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. 2020. The EGRBAC Model for Smart Home IoT. In *2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI)*. IEEE, 457–462.
[2] Nellie Bowles. 2018. Thermostats, Locks and Lights: Digital Tools of Domestic Abuse. https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html
[3] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. 2016. Security analysis of emerging smart home applications. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 636–654.
[4] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. 2018. Rethinking access control and authentication for the home internet of things (IoT). In *27th {USENIX} Security Symposium ({USENIX} Security 18)*. 255–272.
[5] Patrick CK Hung, Kamalakar Karlapalem, and JW Gray. 1998. A study of least privilege in CapBasED-ams. In *Proceedings. 3rd IFCIS International Conference on Cooperative Information Systems (Cat. No. 98EX122)*. IEEE, 208–217.
[6] William Jang, Adil Chhabra, and Aarathi Prasad. 2017. Enabling multi-user controls in smart home devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*. 49–54.
[7] Ravi Sandhu, David Ferraiolo, Richard Kuhn, et al. [n.d.]. The NIST model for role-based access control: towards a unified standard.
[8] Eric Zeng and Franziska Roesner. 2019. Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*. 159–176.