Circles of Trust: A Voice-Based Authorization Scheme for Securing IoT Smart Homes

Jennifer Mondragon
jmondragon6@islander.tamucc.edu
Texas A&M University- Corpus Christi
Corpus Christi, Texas, USA

Gael Cruz
cruzg29@gator.uhd.edu
University of Houston - Downtown
Houston, Texas, USA

Dvijesh Shastri
shastrid@uhd.edu
University of Houston - Downtown
Houston, Texas, USA

Carlos E. Rubio-Medrano
carlos.rubiomedrano@tamucc.edu
Texas A&M University - Corpus Christi
Corpus Christi, Texas, USA

ABSTRACT

Smart homes, powered by a plethora of Internet of Things (IoT) devices, such as smart thermostats, lights, and TVs, have gained immense popularity due to their simple voice command control, making them user-friendly for homeowners and their families. However, these voice commands can be potentially *misused*, especially by unauthorized individuals, like visitors or thieves, who may have not been previously authorized to manipulate security *sensitive* devices, e.g., smart locks. To address this issue, we propose a novel approach called *Circles of Trust* (CoT), rooted in a well-known namesake psychological concept which associates relationships to a specific degree of trust. This concept can be applied to an authorization framework, by linking relationships to an access level, e.g., homeowners and their spouses can be fully-trusted, whereas visitors and children may not. CoT can be further visualized as a multi-layered circle, where the most *privileged* user, e.g., a homeowner, is placed within the innermost layer, and therefore has access to every single device within a smart home via voice commands. Each subsequent layer has fewer access privileges than the previous, granting users in outer layers, like visitors, limited capabilities to manipulate devices. CoT aims to preserve the ease-of-access and convenience of smart home devices by integrating voice-based security policies, eliminating the need for graphical user interfaces (GUIs). The proposed CoT implementation includes three main components: the voice-to-text module, authorization engine, and IoT orchestrator. Following a prototype implementation, a user study and questionnaire will assess the user-friendliness and device convenience.

CCS CONCEPTS

• **Security and privacy → Access control**; • **Human-centered computing → Sound-based input / output**.

KEYWORDS

Smart Homes, Authorization, Access Control, Voice Commands.

SACMAT 2024, May 15–17, 2024, San Antonio, TX, USA

ACM ISBN 979-8-4007-0491-8/24/05
https://doi.org/10.1145/3649158.3657044

ACM Reference Format:
Jennifer Mondragon, Gael Cruz, Dvijesh Shastri, and Carlos E. Rubio-Medrano. 2024. *Circles of Trust*: A Voice-Based Authorization Scheme for Securing IoT Smart Homes. In *Proceedings of the 29th ACM Symposium on Access Control Models and Technologies (SACMAT 2024), May 15–17, 2024, San Antonio, TX, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3649158.3657044

1 INTRODUCTION

The Internet of Things (IoT) facilitates direct information sharing among interconnected devices [6], revolutionizing daily life with smart devices [2]. Smart devices, offering convenience through voice commands, drive the concept of smart home environments, where multiple IoT-connected devices coexist, controlled via a central hub. While voice-command functionality simplifies homeowner tasks, ensuring proper authorization for device usage presents a critical challenge [4]. Implementing hands-free smart home solutions without graphical user interfaces (GUIs) becomes imperative for both usability and security.

In order to address these challenges, we propose a novel solution inspired by the psychological concept of *Circles of Trust* (CoT). The concept of CoT associates relationships within an individual's life with specific levels of trust, represented by circles. By applying this psychological concept to the world of smart home environments, implementations of protection can be completed by requiring an authorization engine to determine if a user is able to execute a command on a specific device. For example, CoT starts with the self layer, centered on an individual, or oneself. Encompassing the self layer, is a layer that is deemed trusted. This layer includes relationships that can be trusted with most sensitive information. The next layer includes the partially trusted level, which can include relationships that can be trusted with some sensitive information. Lastly, the final layer consists of relationships that are considered untrusted, where no sensitive information is shared. A visual representation of these relationship layers is displayed in Figure 1, along with their examples. With this in mind, specific research questions have been curated that aim to evaluate the practicality and effectiveness of voice-based security policies within smart home environments.

- **RQ1:** Can users understand and effectively use voice-based security policies?
- **RQ2:** What specific Smart Home settings may affect the usability of voice-based security policies?

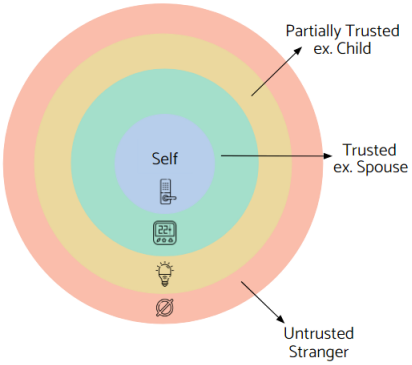

Figure 1: CoT correlates relationships of oneself to layers of trust. The self layer contains all sensitive components, the trusted layer contains few sensitive components, the partially trusted contains non-sensitive components, while the untrusted contains none.

- **RQ3:** Can Smart Home users remember their voice-based security policies over time?
- **RQ4:** Are Smart Home users satisfied with voice-based security policies?

The insights gained from these inquiries will play a crucial role in advancing voice-command policies within the realm of smart homes. The proposed approach will contribute significantly to the understanding of voice-based security policies for Smart Homes.

2 BACKGROUND

The value of smart home device services is widely acknowledged, though it comes with a set of associated risks. Security concerns in smart home devices revolve around various vulnerabilities that can exploit resource constraints and may neglect proper consumer protection measures [9]. Consumer protection involves managing information on devices, where a lack of safeguards raises concerns about privacy violations. Consequently, robust authorization becomes fundamental for securing smart home devices. In addition, authorization and access control play a crucial role in cybersecurity, managing access to sensitive resources within cyber-infrastructures, including software systems. Effective access control involves user-assigned roles and customizable commands for sensitive components, which can be seen in some previous authorization engine works [8]. While authorization engine implementation in smart home devices has been limited, there have been strides to implement a protective base within these devices. Despite these challenges, models such as Role-Based Access Control (RBAC) are renowned for their flexibility and manageability [10]. While RBAC has been explored, challenges exist within the framework when it comes to reliability and scalability [9]. Research on non-interface-based authorization is limited despite the emphasis on access control [3]. Current implementations like Alexa PIN prioritize user protection but fall short in hands-free functionality [11]. Moreover, IoT-powered smart home devices have explored access control methods, but the integration of a GUI adds complexity causing burdens to users by hindering convenience and reducing scalability. In multi-occupant setups, current access models often stumble without GUIs, highlighting the need for a flexible authorization engine for voice-based security in smart home environments.

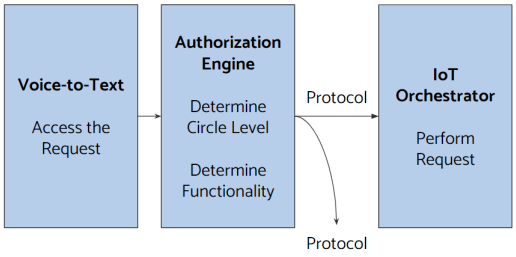

Figure 2: The components of CoT: the voice-to-text component, responsible for handling spoken content; the authorization engine, managing access levels and associated functions; and the IoT orchestrator, which executes access commands.

3 METHODOLOGY

This paper proposes CoT, integrating the psychological concept of Circles of Trust into smart home devices to address the lack of authorization schemes while retaining voice command simplicity. Inspired by Dunbar et al.'s work [7], CoT establishes trust levels among household members, adapting the concept to IoT for varied levels of trust which is displayed in Figure 1. Prioritizing flexibility and scalability, homeowners can customize access levels and commands, facilitated by an engine managing roles and execution status. GUI absence ensures device convenience, with voice-based security policies efficiently handling commands. Additionally, the authorization flow involves voice-to-text and IoT orchestrator components. The conceptual figure presented by Figure 2, outlines the key components and interactions within the proposed system.

Voice-to-Text. Utilizing the Google Speech-to-Text API, essential for CoT functionality, involves converting spoken words into text for command processing [1]. This API streamlines the process by enabling real-time transcription, which can be later used for command execution based on access levels without the need for additional integration.

Authorization Engine. The authorization engine serves as the scheme's core, handling user roles, permissions, and scalability considerations. Homeowners can assign permissions directly or opt for default settings, facilitating straightforward household member management and ensuring scalability. Access levels—self, trusted, partially trusted, and untrusted—are tailored to device sensitivity and homeowner preferences. A visualization of possible device access roles is provided in Table 1. Python is chosen for its readability and extensive library support, with initial development focusing on role-based class creation. The preliminary stages of implementation will center around developing classes that represent distinct roles within the household, each associated with well-defined access levels and corresponding commands. This structured approach not only enhances clarity but also sets the stage for scalable and robust functionality in the evolving realm of smart home technology.

IoT Orchestrator. The IoT orchestrator, the final stage for command execution, relies on the user's request and their access level. Seamless integration between the authorization engine and the

Table 1: *Access Levels & Sensitivity for Example Devices.*

Example Device	Sensitivity	Roles
Smart Lock	High	Homeowner
Smart Thermostat	Medium	Homeowner Trusted
Smart Light	Low	Homeowner Trusted Partially Trusted
No Device	None	Untrusted

voice-to-text module ensures protocol execution. Device orchestration is closely tied to user roles; if a role restricts a command, the protocol halts before involving the IoT orchestrator. Successful implementation hinges on the choice of SDK and specific smart devices, but varying APIs based on individual devices pose integration challenges due to the lack of a universal standard in smart device development. Tuya is widely acknowledged in the IoT industry, especially for smart home devices, as its API is easily accessible and Tuya maintains robust linking capabilities [12]. In some cases, various IoT devices from differing companies utilize Tuya, making it possible to handle various devices within the home under one framework. To implement the IoT orchestrator, we will use TinyTuya, a Python package to control and read the current state of devices, streamlining the IoT orchestration [5].

4 EXPECTED RESULTS

The anticipated results will demonstrate CoT's compliance and assess its impact on latency, scalability, and flexibility. A user study will evaluate its effectiveness in various home environments, followed by a questionnaire comparing CoT with traditional authorization methods to refine the model and enhance user experience.

Performance. Evaluation of the authorization engine's performance and adaptability is crucial for ensuring seamless integration within smart home environments. This comprehensive assessment ensures that the authorization engine meets performance standards while adapting seamlessly to evolving smart home environments. Whether the authorization engine operates in the cloud or locally, assessing latency and processing time is essential. Excessive delays can undermine the convenience of smart devices, necessitating alignment with base smart home technology.

Scalability. Scalability assessment focuses on the system's ability to accommodate new users, devices, and commands. The engine must effectively manage multi-occupant homes with varying access levels and devices. Understanding and utilizing voice-based policies, along with policy retention over time, are key scalability considerations. User feedback from studies and questionnaires will provide insights into scalability effectiveness.

Flexibility. Flexibility evaluation revolves around homeowners' ability to customize access controls based on home roles. Insights gained from user studies and questionnaires will highlight understanding and utilization of voice-based security policies, policy retention, and satisfaction with the authorization engine's results. Compatibility issues with varying smart home settings may influence flexibility, warranting consideration in the evaluation process.

User Study. Including a user study is essential to evaluate the effectiveness of the authorization scheme. A baseline trial will gather information on device misuse and traditional approaches, providing insights into the benefits of CoT. Following this, an experimental trial consisting of at least two runs separated by a week and then a month will assess immediate and long-term responses, ensuring the security and functionality of CoT. A questionnaire administered to study participants will assess the benefits of CoT, as well as mental and physical workloads associated with its usage. It will compare user perceptions of CoT with traditional GUI-based approaches, shedding light on its alignment with the ideal user experience, and providing essential insights for further developments.

5 CONCLUSION

The expansive market of smart devices, though incredibly accessible and convenient, still struggles with significant challenges in terms of privacy and security. Existing research predominantly focuses on authorization with GUIs, yet there remains a notable gap in the implementation of robust authorization schemes that use solely voice. The CoT approach should not only maintain the seamless and convenient nature of smart devices but alleviates the burden associated with authorization through GUIs while prioritizing protection, which can contribute to security of smart devices by enhancing convenience and accessibility for smart households.

ACKNOWLEDGMENTS

This work was partially supported by the CAHSI-Google Institutional Research Program, sponsored by Google Inc. and the Computing Alliance of Hispanic-Serving Institutions (CAHSI), a National Science Foundation (NSF) INCLUDES Alliance.

REFERENCES

[1] 2024. (2024). https://cloud.google.com/speech-to-text.
[2] Noura Abdi, Xiao Zhan, Kopo M. Ramokapane, and Jose Such. 2021. Privacy norms for smart home personal assistants. In *Proc. of the 2021 CHI Conference on Human Factors in Computing Systems* (CHI '21) Article 558. Association for Computing Machinery, New York, NY, USA, 14 pages.
[3] Bogdan Cosmin Chifor, Ion Bica, Victor Valeriu Patriciu, and Florin Pop. 2018. A security authorization scheme for smart home internet of things devices. *Future Generation Computer Systems*, 86, (Sept. 2018), 740–749. DOI: 10.1016/j.future.2017.05.048.
[4] Luís Costa, Joao Paulo Barros, and Miguel Tavares. 2019. Vulnerabilities in iot devices for smart home environment. *ICISSP 2019 - Proc. of the 5th International Conference on Information Systems Security and Privacy*, 1, 1, 615–622.
[5] Jason Cox. 2023. Tinytuya. https://github.com/jasonacox/tinytuya. (2023).
[6] Brittany D. Davis, Janelle C. Mason, and Mohd Anwar. 2020. Vulnerability studies and security postures of iot devices: a smart home case study. *IEEE Internet of Things Journal*, 7, (Oct. 2020), 10102–10110, 10, (Oct. 2020). DOI: 10.1109/JIOT.2020.2983983.
[7] R. I. Dunbar. 2008. Cognitive constraints on the structure and dynamics of social networks. group dynamics: theory, research, and practice. (2008).
[8] M. Ebrahim Abidi, Ani Liza Asnawi, N.FM. Azmin, A.Z. Jusoh, S. Noorjannah Ibrahim, Huda Adibah Mohd Ramli, and Norun Abdul Malek. 2018. Development of voice control and home security for smart home automation. In *2018 7th Int. Conf. on Computer and Communication Engineering (ICCCE)*, 1–6.
[9] Ziarmal Nazar Mohammad, Fadi Farha, Adnan O M Abuassba, Shunkun Yang, and Fang Zhou. 2021. Access control and authorization in smart homes: a survey. (2021). www.apple.com/ios/home/.
[10] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman. 1996. Role-based access control models. *Computer*, 29, 2, 38–47. DOI: 10.1109/2.485845.
[11] Marinel Sigue. 2023. Google home voice match: what it is and how to use it. (Jan. 2023). https://www.makeuseof.com/what-is-google-home-voice-match/.
[12] Tuya. 2023. Tuya smart - global iot developer service provider. https://www.tuya.com. (2023).