Poster: Leveraging Interpersonal Dynamics for IoT Privacy

Nathan Malkin, Alan F. Luo, Julio Poveda, Michelle L. Mazurek
University of Maryland
{nmalkin,alanfluo,jpoveda,mmazurek}@umd.edu

Abstract—**Smart home devices are well-known to create privacy tensions in households. To address these, users frequently express preferences for complex access control policies, but in practice they often settle for less secure defaults. As an alternative, we investigate access control policies that allow users to select their desired level of access, subject to oversight from other household members. This solution allows users to leverage the interpersonal trust they already rely on in order to establish privacy boundaries commensurate with more complex access control methods, while retaining the convenience of less secure strategies. Because this approach is subject to inherent security and privacy tradeoffs, our research is focused on investigating the acceptability and perceptions of this approach for end-users.**

1. Introduction

Interpersonal privacy is a significant concern in smart homes [7], [14]; as a result, access control is often a required feature for Internet of Things (IoT) devices. Many solutions have been proposed, both as research prototypes [4], [12], [14] and in deployed systems [5], [13]. A common assumption is that each individual has their own account, which is not shared. In practice, such assumptions often turn out to be false: a frequent phenomenon is for multiple users to share the same account and password for a single device [8]. Even when access control schemes are designed with usability in mind, users choose to ignore complex configuration options, reporting that they trust their cohabitants and preferring to mediate access through existing interpersonal dynamics, rather than mechanical access control methods [14].

The status quo is therefore contradictory: on one hand, researchers document privacy violations that are enabled by smart devices [1], [3], and users express a desire for more controls that can help address these [6]. On the other hand, they also appear reluctant to adopt systems that would allow for such granular access control. A major reason for this may be usability: creating accounts and defining access control policies require a significant time investment, and the benefits may be unclear or non-existent [11]. Furthermore, users may be unwilling to adopt rigid policies due to concerns about unanticipated access needs and unplanned situations [9]. Because they generally trust others in their household, users prefer more flexible schemes and arrangements.

We hypothesize that, rather than acting strictly as barriers, these constraints can be leveraged to create new, more practical, user management techniques for smart home devices. We therefore propose a novel scheme and argue for why it may be a good fit for today's household environments.

2. Approach

Our approach is inspired by prior literature on "optimistic access control" (OAC) [2], [10]. In lieu of immutable policies, we propose allowing people to obtain the level of access that they think they need, but providing sufficient visibility so that inappropriate access can be detected by others in the household. The knowledge that others may find out, and the user will have to face consequences, might be a sufficient deterrent for people not to exceed their authorization without good reason.

Concretely, "optimistic" ideas can be applied to the IoT user experience as follows: when someone new wants to start using a smart device in their home, they can do this without obtaining prior authorization, for example by scanning or entering a code visible on or near the device. However, this access is subject to oversight: any existing user will receive a notification about the new one through their app, which allows them to revoke or otherwise manage the new person's access if they have concerns. This method is equivalent in its convenience to having a single account and posting its credential publicly, but by assuming each new enrollment is potentially a different user, it allows for better-defined privacy boundaries, for example, by compartmentalizing each user's data. Another manifestation of optimistic ideas could be to allow users to review data collected by the device—again, without special approval—but anyone whose data they review as part of this process will be notified.

We believe that the optimistic model is a good fit specifically for user management in many smart homes. People already display high levels of interpersonal trust, as evidenced by the popularity of account sharing. But they do have norms and expectations, which can be hard to codify in formal access control policies. With OAC, users are freed from this chore. If misbehavior occurs, they can rely on existing methods of sanctioning it and resolving disputes.

3. Research questions

While OAC offers convenience by removing upfront fine-grain configuration and user management, it carries a significant set of tradeoffs in its approach to security and privacy. Security is not as strong in OAC as in a system with traditional access control settings, because access can be obtained without prior authorization, which can be exploited by people inside and outside the household. On the other hand, OAC's security is better compared with the default of everyone using the same account, because different people can have different access levels. Similarly, OAC may be beneficial to privacy, since access notifications may deter some people from snooping. But the activity notifications themselves can serve as a privacy leak.

In our research, we have set out to test our hypothesis by studying if—and when—OAC is a good match for smart homes. We begin by focusing on people's perceptions of this new approach in order to understand users' reactions and likelihood of adoption, if it were offered in real products.

4. Methods

To begin answering our research questions, we conducted a survey study with approximately four hundred participants, examining their preferences and opinions about optimistic access control. After asking about current sharing practices, we presented participants with a description of an access control mode that relied on optimistic principles as well as two other modes that represented the status quo. We asked people to select among the modes for two different device types as well as to explain their reasoning through open-ended responses. We additionally asked participants to rate the modes on their convenience and security or privacy as well as collecting potential concerns.

We chose to study two different contexts in which optimistic access control may be a good fit: determining (1) who has access to control a device and (2) who can review data on the device. In the first context ("onboarding"), we decided that any time a user accessed a device for the first time, this event merited auditing. The auditors would be all existing members of the household with access to that device. In contrast, in the "review" context, we posited that the person doing the auditing should be the one whose data is being accessed, and that they would be invited to do this each time their data was accessed.

5. Key results

When asked about how they currently manage shared devices, approximately two thirds of our participants reported that they use a single account, shared by all household users. This serves as a crucial reminder that account sharing—despite its many security and privacy drawbacks—represents the default for many users; any alternatives will need to draw users away from this choice. To that end, our study found that optimistic access control was moderately successful: a plurality of respondents still preferred to share a single account, but up to a third chose OAC as their preferred way of sharing devices, finding that its security was higher and its convenience was on par. A regression showed that this preference varies significantly by device type, and that other contextual factors, such as the number of devices owned and household composition, may play a role as well.

References

[1] Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster. Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic. *arXiv preprint arXiv:1708.05044*, 2017.

[2] Bob Blakley. The emperor's old armor. In *Proceedings of the 1996 Workshop on New Security Paradigms*, NSPW '96, pages 2–16, New York, NY, USA, 1996. Association for Computing Machinery.

[3] Camille Cobb, Milijana Surbatovich, Anna Kawakami, Mahmood Sharif, Lujo Bauer, Anupam Das, and Limin Jia. How risky are real users' IFTTT applets? In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 505–529. USENIX Association, August 2020.

[4] Sofia Dutta, Sai Sree Laya Chukkapalli, Madhura Sulgekar, Swathi Krithivasan, Prajit Kumar Das, and Anupam Joshi. Context sensitive access control in smart home environments. In *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pages 35–41. IEEE, 2020.

[5] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. Security analysis of emerging smart home applications. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 636–654. IEEE, 2016.

[6] Christine Geeng and Franziska Roesner. Who's In Control?: Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, pages 268:1–268:13. ACM, 2019.

[7] Weijia He, Valerie Zhao, Olivia Morkved, Sabeeka Siddiqui, Earlence Fernandes, Josiah Hester, and Blase Ur. SoK: Context sensing for access control in the adversarial home IoT. In *2021 IEEE European Symposium on Security and Privacy (EuroS p)*, pages 37–53, 2021.

[8] William Jang, Adil Chhabra, and Aarathi Prasad. Enabling multi-user controls in smart home devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, pages 49–54, 2017.

[9] Michelle L. Mazurek, Peter F. Klemperer, Richard Shay, Hassan Takabi, Lujo Bauer, and Lorrie Faith Cranor. Exploring reactive access control. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2085–2094, Vancouver BC Canada, May 2011. ACM.

[10] Dean Povey. Optimistic security: A new access control paradigm. In *Proceedings of the 1999 Workshop on New Security Paradigms*, NSPW '99, pages 40–45, New York, NY, USA, 1999. Association for Computing Machinery.

[11] Robert W Reeder, Lujo Bauer, Lorrie F Cranor, Michael K Reiter, and Kami Vaniea. More than skin deep: Measuring effects of the underlying model on access-control system usability. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2065–2074, 2011.

[12] Amit Kumar Sikder, Leonardo Babun, Z. Berkay Celik, Abbas Acar, Hidayet Aksu, Patrick McDaniel, Engin Kirda, and A. Selcuk Uluagac. Kratos: Multi-user multi-device-aware access control system for the smart home. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 1–12, Linz Austria, July 2020. ACM.

[13] Blase Ur, Jaeyeon Jung, and Stuart Schechter. The current state of access control for smart devices in homes. In *Workshop on Home Usable Privacy and Security (HUPS)*. HUPS 2014, July 2013.

[14] Eric Zeng and Franziska Roesner. 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)*, pages 159–176, Santa Clara, CA, August 2019. USENIX Association.