A Community-based Approach to Co-Managing Privacy and Security in Smart Homes

ERIC BURDEN, BSIT, University of Cincinnati, United States
RAJDEEP BRANDOPADHAYAY, University of Cincinnati, United States
NATHAN J. ELROD, MSIT, University of Cincinnati, United States
SHANE HALSE, PhD, University of Cincinnati, United States
JESS KROPCZYNSKI, PhD, University of Cincinnati, United States

ABSTRACT

This study proposes enhanced oversight of smart homes by leveraging the social networks of homeowners to co-monitor for emergencies, while being mindful of privacy preserving features necessary for adoption. A pilot co-design workshop was conducted to determine features for co-monitoring. A group of four participants provided early findings and informed modifications to study design, and new insights for user behavior were emphasized. By refining the study design, we hope to better target users' tacit knowledge in future workshops. Early findings include the users' need for more than simply sharing access to a camera during an emergency in the home; users desired control over the microphone, the camera video stream, and the length of time. We believe this work will contribute to a broader understanding of features that better meet the needs and goals of smart device owners to enable co-monitoring.

CCS Concepts: • **Security and privacy → Human and societal aspects of security and privacy → Usability in security and privacy; •Human-centered computing → Interaction design.**

Additional Key Words and Phrases: IoT security and privacy, access control, application co-design

ACM Reference Format: Eric Burden, Rajdeep Brandopadhayay, Nathan J. Elrod, Shane Halse, and Jess Kropczynski. 2020. A Community-based Approach to Co-Managing Privacy and Security in Smart Homes. In *IT Research Symposium '20: School of Information Technology IT Research Symposium, April 14, 2020, Cincinnati, OH*, USA, 6 pages.

1 Introduction

The proliferation of smart homes over the last decade has seen research focus primarily on the technological and security aspects of IoT devices [1, 2]. Smart homes today lack effective methods for co-monitoring or the ability to share access of connected devices; privacy is seen as an all-or-nothing approach, and rarely takes environmental factors into account as applied to access controls [3, 5]. Prior work shows that smart home users desire more complex threat detection and response mechanisms than current offerings [3, 4, 18]. By defining the user experience needs of families and other tight-knit social groups during an emergency event in the home, we can potentially facilitate easier co-monitoring of the smart home. This paper specifically focuses on the social constraints and technological needs of smart home users when co-monitoring for emergencies. We aim to probe how

IT Research Symposium '20, April 14, 2020, Cincinnati, OH

users might approach sharing access to smart devices in their home to determine threats and make safety decisions by providing their social networks access to the smart home.

We used a co-design methodology to help study the tacit knowledge used by smart homeowners in home security decision-making. We chose this focus because tacit knowledge - what people know without being able to articulate - is typically difficult to formalize and describe [11]. By allowing the individuals in this study to co-develop portions of an app, a more focused idea of their expectations might emerge. This paper reviews the overall study design of this work and presents the early results from a pilot round of data collection. Feedback from the users presented ideas such as: sharing access for limited and short amounts of time; notifying all members of the group simultaneously, instead of sequentially; and organizing devices by room when sensors detect potential threats to the smart home.

2 Related Work

Smart homes are populated by devices 'incorporating smartness' into dwellings through automation, AI, location awareness, and virtual assistants. These smart devices allow for increased personal comfort, safety, security, as well as device monitoring and energy conservation [14]. The smart home is an intelligent system that dynamically responds to the behavior of residents in personalized ways, both direct and indirect [21].

In 2016, one-in-eight American homes could be classified as 'smart homes.' With the widespread adoption of Internet of Things (IoT) technologies as homeowners rapidly join the smart home space, that number is expected to grow to almost one-in-three homes by 2021 [10]. During this rapid growth of the IoT, there exists no industry-wide or cross-platform solution for these devices to be shared easily; considering the Internet of Things was partially derived from a desire to share data and improve decision making using that data, this is a major concern for the future of the IoT [15]. Additionally, when considering access control most research focuses on accessing the data of a smart home, primarily of multimedia or data files (e.g. music files and personal information), replication of an individual's data, or that each device can or might have a need to replicate data [7, 8, 9].

A limiting assumption is that devices and the smart home are essentially "single-user" [3, 6]. While current access controls in smart homes are often device centric, a user study from He et al. [3] demonstrated that users desire capability and relationship-centric models for access control, since there are often multiple ways a task can be completed. When seeking to co-monitor in the instance of events such as fires, floods, or burglaries, these devices must be controlled using multiple applications that unnecessarily complicate the user experience, and further limit each individual system as a part of the smart home. Typically, smart home devices are placed in a shared environment and used by multiple people. This is different from previous technological and personal device innovations, such as laptops and smartphones, where the primary user was typically the only user.

Smart homes can have a number of privacy concerns, such as how data and device access is controlled between household members. He et al. found that multi-user smart home consumers would prefer control at function-level granularity rather than per-device access control [3]. User privacy, or the "control over personal information" [16], is another concern for smart homes in particular. Prior work has explored in-home privacy from third parties such as device manufacturers, advertisers, and the government [17, 18]. The home is regarded as a private and personal space, with multiple stakeholders that have competing needs and tolerance for what is considered acceptable and useful data sharing. Choe et al. [19] surveyed homeowners for the needs and concerns of activities and habits that people have at home that they would not want recorded; however, the participants did not explicitly state who could have access to recordings. For example, parents want to monitor their children, but also

want to respect their privacy when recording [20]; the same concerns exist around smart home devices for elder care or older adults. Smart home devices in shared physical spaces will further press on these issues. Even non-household users - people that are just visiting the home or are a guest - might have the same concerns for privacy and recordings in a smart home.

3 Problem Statement and Research Questions

This project will explore social aspects of smart home technology and access control. By studying how smart home users can implement different access control policies and emergency notification systems, we aim to enhance the privacy and security of smart homes and smart devices.

As follows from the background literature, the use of IoT devices in smart homes is on the rise [10] and these devices may provide increased home security when monitored consistently. Co-monitoring may help in this regard, but devices lack the nuanced access control described by consumers [3]. Therefore, this study aims to understand ways to design nuanced access controls to enable co-monitoring of smart homes.

To address the previously stated problem, this work takes an exploratory, grounded approach to answer the following research questions:

RQ1: What mobile app features can homeowners, friends, and family members use to co-monitor threats in-case-of-emergency to a smart home while still protecting the privacy of homeowners?

RQ2: What design specifications are needed to support the information requirements in a mobile application to share access to personal devices with family and friends?

4 Methods

Using a co-design study to develop an interface for sharing access and notifying the monitoring members, we can explore the thoughts and methods people naturally use for interactions with others during their use of smart devices [9]. We chose a co-design to focus on tacit knowledge - what people know without being able to articulate – because it is difficult to formalize and describe this knowledge [11]. While utilizing the tacit knowledge of these individuals through the recording of trends in interface needs and instinctive workflow, the interface can better meet the needs and goals of smart device owners; this will enable co-monitoring that protects the home while still protecting the privacy of the occupants. By observing discussions and features selected for this interface, we aim to increase our understanding of the underlying tacit knowledge individuals hold about smart device access control and how they might share it while preserving privacy; after approximately fifteen groups of 3-4 participations, we will determine trends in the features users deem necessary in a smart home access control management interface. Using our collected data we will devise an interface that will effectively allow smart homeowners to share access to their social networks.

Subjects will be recruited using multiple methods such as posting on social media, posting flyers on college campuses as well as contacting families known to team members, and families of the team members themselves; recruitment will take place through the spring semester as well as the beginning of the summer semester. The subjects recruited online will be asked to submit an application through a form with a group of 3-4 people (friends, family) After determining their eligibility, they will be asked for consent and a time will be set-up to conduct the study. The expected duration of subject participation in the study is about 60 minutes.

Previous work in the IoT space for co-designing an app used methods from participatory design. Chouhan et al. [22] used this method to test an application that would support community collaboration. This study will not provide a working prototype; instead, participants will be asked to examine and practice IoT co-monitoring, and to consider themselves as either a homeowner or guest in a residential setting with pre-existing and initialized IoT devices. Participants are then given the task of designing tools to maximize benefits and mitigate concerns in scenarios such as a fire, burglary, or flooding. The interviewer will ask questions about how they might want to share smart device access with their social networks in order to effectively deal with the threat.

An interviewer presents an activity to engage individuals and social groups (focusing on nuclear families, friends, and other tight knit groupings) from the local community in a discussion of primary features to be used to design a smart home co-monitoring smartphone application. We will examine how residents of smart homes might implement access controls throughout a smart home by walking them through a series of storyboards to demonstrate how co-monitoring of smart home devices can benefit users, or inadvertently compromise privacy. In these scenarios, we want to understand the access they are willing to share (for example, sharing the ability to shut off a smart water main in the event of a flood) and how they might design an app to provide access to their social network to co-monitor threats to their home. Participants' story board reaction and social group interactions will be collected through notes and recordings.

While they perform these tasks, we will be observing the participants and taking notes about their interactions and their comments. The interviewer will then ask the group to build their own app, and provide them UI elements (e.g. icons, app elements, app screens and pages, and other app functions) to build their desired application interface. This will be a low fidelity prototype on paper – for example, a mockup of a blank iPhone with a bucket of random UI icons, textboxes, elements. The interviewer will guide the homeowners through a scenario, ask them what they expect to see (how they would assemble the screen and features to execute the task), then follow up with the other users (peripheral users) to determine how they would expect a notification to appear. Users will be focusing on sharing data access and with whom, and responding to the threats; as such, the important information to collect is interactions with the interface and what data is actively shared.

5 Early Findings

A pilot study comprising a group of four volunteers gave us several early insights into user preferences for the application. Several common themes arose amongst the participants, as well as some unique ideas. The group first designed a screen to enable sharing with multiple people that included a contacts page with a section at the top for favorites which would enable users to quickly add frequently contacted people. Participants also wanted to have a slider bar where you could set different emergency levels; these levels would then be used to determine if it is appropriate to give other people access.

Users also wanted to be able to share access to their smart speakers' microphones in case of burglaries for the ability to 'listen in'. Other requested features included having fail-safes in place for false alarms. Such fail-safes would be implemented by giving people temporary access until an 'event' was in progress and would let homeowners know when someone was accessing their devices. Generally, the overall flow of tasks was different from what we expect; refinements in questions were drawn from the feedback provided during this pilot.

6 Conclusion

This study is currently under review by the University of Cincinnati Institutional Review Board and recruitment of participants will commence upon approval. We believe this work will contribute to a broader understanding of features that can be used to implement co-monitoring of smart homes while also being careful to consider privacy preserving elements in the design.

Since we are focusing on collecting the users' tacit knowledge, our methods have been refocused after our initial pilot study. We are attempting to emulate the flow and use of implicit usability desires for certain specific cases demonstrated in our storyboards. By creating opportunities for users to describe their knowledge, it can be used to design new tools and workflows that provide users with the features they desire. The result of this work is to come up with a guideline for the best feature-set to facilitate access sharing for certain smart home emergency scenarios. From our initial pilot, it appears that our study design will be successful in in this task.

Our future work can be broken down into a 3-stage process. Starting with the Exploration stage, the user (participants) will be familiarized with the application by designers who act as mediators. The user is familiarized with the procedure and is assigned certain goals they are supposed to work on. In the next stage, Discovery, designers and users work closely to iteratively employ a number of features to achieve the given goal and understand the priorities for both parties and get a better and more refined architecture based on the co-design results created at the study's outcome. During this study phase our intent is not to bias the users toward a certain design or feature since our primary goal is to collect the users' tacit knowledge and capture the feature set that fits their needs best. Stage three is Prototyping, which involves an iterative approach to deploy a co-design prototype that is based on the data collected in stage one and two. After testing against the theories and results from the previous stages, we will attempt to full answer the needs of smart home access control and co-monitoring.

ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under Grant No. 1814110 and by the Mozilla Research Foundation. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation or the Mozilla Research Foundation.

REFERENCES

[1] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y. (2017). Understanding the mirai botnet. In *26th {USENIX} Security Symposium ({USENIX} Security 17)* (pp. 1093-1110).

[2] Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security analysis of emerging smart home applications. In *2016 IEEE Symposium on Security and Privacy (SP)* (pp. 636-654). IEEE.

[3] He, W., Golla, M., Padhi, R., Ofek, J., Dürmuth, M., Fernandes, E., & Ur, B. (2018). Rethinking access control and authentication for the home internet of things (IoT). In *27th USENIX Security Symposium (USENIX Security 18)* (pp. 255-272).

[4] Agrawal, D., Bhagwat, R., Bandopadhyay, R., Kunapareddi, V., Burden, E., Halse, S., Wisniewski, P., & Kropczynski, J. (2020, January). Enhancing Smart Home Security using Co-Monitoring of IoT Devices. In Companion of the 2020 ACM International Conference on Supporting Group Work (pp. 99-102).

[5] Geeng, C., & Roesner, F. (2019, May). Who's In Control? Interactions In Multi-User Smart Homes. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (pp. 1-13).

[6] Lekakis, V., Basagalar, Y., & Keleher, P. (2012, June). Don't trust your roommate or access control and replication protocols in" Home" environments. In Proceedings of the 4th USENIX conference on Hot Topics in Storage and File Systems (pp. 12-12).

[7] Mazurek, M. L., Arsenault, J. P., Bresee, J., Gupta, N., Ion, I., Johns, C., Lee, D., Liang, Y., Olsen, J., Salmon, B., & Shay, R. (2010, April). Access control for home data sharing: Attitudes, needs and practices. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 645-654).
[8] Andaloussi, Y., El Ouadghiri, M. D., Maurel, Y., Bonnin, J. M., & Chaoui, H. (2018). Access control in IoT environments: Feasible scenarios. Procedia computer science, 130, 1031-1036.
[9] Ouaddah, A., Mousannif, H., Elkalam, A. A., & Ouahman, A. A. (2017). Access control in the Internet of Things: Big challenges and new opportunities. Computer Networks, 112, 237-262.
[10] Paxton, M. (2017, June 14). Smart Homes In The U.S. Becoming More Common, But Still Face Challenges. Retrieved March 7, 2020, from https://www.spglobal.com/marketintelligence/en/news-insights/blog/smart-homes-in-the-u-s-becoming-more-common-but-still-face-challenges
[11] Spinuzzi, C. (2005). The methodology of participatory design. Technical communication, 52(2), 163-174.
[12] Tabassum, M., Kropczynski, J., Wisniewski, P., and Lipford, H.R. (Accepted for 2020) Smart Home beyond the Home: A Case for Community-based Access Control. In Proceedings of CHI'2020
[13] Ur, B., Jung, J., & Schechter, S. (2013, July). The current state of access control for smart devices in homes. In Workshop on Home Usable Privacy and Security (HUPS) (Vol. 29, pp. 209-218). HUPS 2014.
[14] Alam, M. R., Reaz, M. B. I., & Ali, M. A. M. (2012). A review of smart homes—Past, present, and future. IEEE transactions on systems, man, and cybernetics, part C (applications and reviews), 42(6), 1190-1203.
[15] Coetzee, L., & Eksteen, J. (2011, May). The Internet of Things-promise for the future? An introduction. In 2011 IST-Africa Conference Proceedings (pp. 1-9). IEEE.
[16] Solove, D. J. (2008). Understanding privacy.
[17] Pew Research Center. (2016). Privacy and Information Sharing Report. Retrieved 2020-03-08 from http://www.pewinternet.org/2016/01/14/scenario-home-activities-comfort-and-data-capture/
[18] Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. Proceedings of the ACM on Human-Computer Interaction, 2(CSCW), 1-20.
[19] Choe, E. K., Consolvo, S., Jung, J., Harrison, B., & Kientz, J. A. (2011, September). Living in a glass house: a survey of private moments in the home. In Proceedings of the 13th international conference on Ubiquitous computing (pp. 41-44).
[20] Choe, E. K., Consolvo, S., Jung, J., Harrison, B., Patel, S. N., & Kientz, J. A. (2012, September). Investigating receptiveness to sensing and inference in the home using sensor proxies. In Proceedings of the 2012 ACM Conference on Ubiquitous Computing (pp. 61-70).
[21] Lobaccaro, G., Carlucci, S., & Löfström, E. (2016). A review of systems and technologies for smart homes and smart grids. Energies, 9(5), 348.

[22] Chouhan, C., LaPerriere, C. M., Aljallad, Z., Kropczynski, J., Lipford, H., & Wisniewski, P. J. (2019). Co-designing for Community Oversight: Helping People Make Privacy and Security Decisions Together. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), 1-31.