Enhancing Smart Home Security using Co-Monitoring of IoT Devices

Dev Agrawal
University of Cincinnati
Cincinnati, OH 45220, USA
agrawadv@mail.uc.edu

Rahul Bhagwat
University of Cincinnati
Cincinnati, OH 45220, USA
bhagwarl@mail.uc.edu

Rajdeep Bandopadhyay
University of Cincinnati
Cincinnati, OH 45220, USA
bandoprp@mail.uc.edu

Vineela Kunapareddi, MSIT
University of Cincinnati
Cincinnati, OH 45220, USA
vineela.kunapareddi@uc.edu

Eric Burden
University of Cincinnati
Cincinnati, OH 45220, USA
burdenea@mail.uc.edu

Shane Halse, PhD
University of Cincinnati
Cincinnati, OH 45220, USA
shane.halse@uc.edu

Pamela Wisniewski, PhD
University of Central Florida
Orlando, FL 32816, USA
pamwis@ucf.edu

Jess Kropczynski, PhD
University of Cincinnati
Cincinnati, OH 45220, USA
jess.kropczynski@uc.edu

GROUP'20 Companion, January 6–8, 2020, Sanibel Island, FL, USA.
Copyright © 2020 Copyright is held by the owner/author(s).
ACM ISBN 978-1-4503-6767-7/20/01.
https://doi.org/10.1145/3323994.3369883

Abstract

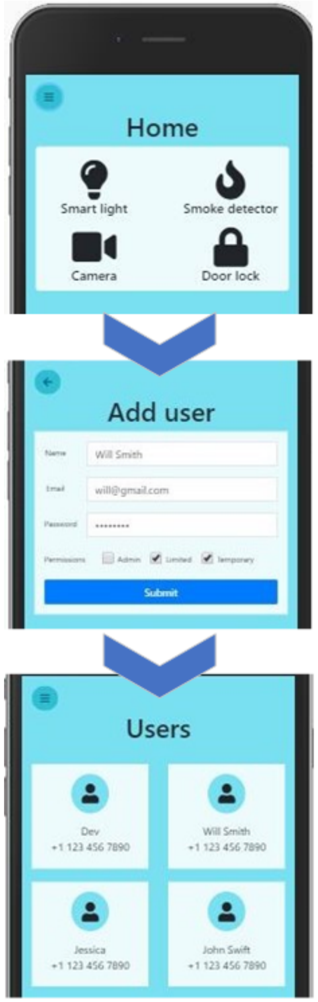
The Internet of Things (IoT) has improved home security for users at home and away, however, most smart home notification systems fail to recognize whether a user has responded to threats in their home. Allowing multiple users to receive alerts can alleviate this issue, but some smart home owners would prefer to limit access controls to "in case of emergency" access. This study explores smart home hub features to co-monitor IoT device access through Role and Event Based Access Control (REBAC), leveraging a device owner's social network, i.e. neighbors and relatives, when homeowners are not available or have failed to respond to a potential threat. Our findings of user studies with two pilot groups demonstrated user's willingness to share access to their smart homes, provided access controls had limited permissions. By adding contextual information of an event to traditional access control models, we were able to create richer permission protocols.

Author Keywords

Internet of Things; Smart Home; Access Control; Permission Management; Home SecuritySmart home; IoT; access controls; user study

Introduction

Interconnected Internet of Things (IoT) devices are capable of automation and enhanced monitoring. Often connected



Name Will Smith
Email will@gmail.com
Password ********
Permissions ☐ Admin ☑ Limited ☑ Temporary

Dev +1 123 456 7890
Will Smith +1 123 456 7890
Jessica +1 123 456 7890
John Swift +1 123 456 7890

Figure 1: ThingZone User Configuration Screens

and managed through a central hub, this network of devices has been termed a "smart home". The affordances of these devices has led to their increased use in recent years and continued use is predicted [6]. Previous research in the domain of IoT security and privacy focuses on cyber-threats and software vulnerabilities [7, 8], we further this work by investigating secure access-control methods. Currently, most smart homes lack the capability to share temporary device access, and are single-user entities that discourage collaborative home monitoring when the resident is away through ridged all-or-nothing access to data and controls.

Previous research has examined the types of social roles IoT users are willing to share access with [5]. We extend this work by implementing an access management system into a smart home hub and observe how users collaboratively deal with a simulated threat. We believe a truly "smart" home is a flexible access-control system that is simple and intuitive to set up. This system should allow outside assistance when owners are otherwise occupied. Our main focus is emergency detection, notification, and response, granting temporary emergency access to relatives and neighbors.

Research Question

We have posed an overarching research question to help us evaluate IoT hub access control infrastructure and supporting tools: *What are the best methods to implement temporary access control of smart homes to ensure effective co-monitoring and handling of threats?*

Research Methods

The preliminary investigation of this question has been through pilot lab testing with two user groups of 3 and 4 people. The studies employed Scenario-Based Design [3] that presented users with a high fidelity prototype written in HTML and JavaScript in order to test and refine the overall information flows, and notification texts. The insights gathered in this study were used to improve the functionality and interface of the prototype and added to the design specifications for our implementation, called *ThingZone*.

The main objective of the first user study was to determine people's preferences pertaining to shared access of their devices in the IoT. To do this, we invited small student groups to engage in role-playing activities with each person assuming a specific role in the group (smart home owner/hub administrator, close friend, and neighbor). The home owner was asked to consider two types of smart home threat scenarios: a fire and unusual upload activity on their home network. They were then asked to begin using the app by sharing access to IoT devices in a way that would help them mitigate these threats. Users first added devices to the smart home hub using the Home Screen (see Figure 1, top) and then added users and their degree of access to these devices (see Figure 1, middle and bottom). While doing so, users were asked to think aloud about their thoughts and concerns about adding a friend or neighbor.

After the administrator completed configuration of the smart home, the two threat scenarios were enacted through a series of drills.

Initial Findings

Described here are initial findings from observation of two pilot groups organized by tasks assigned to the users.

Task 1. Configuring the Smart Home: After the administrator role registered a smart home, added some virtual devices, and created accounts for others along with access permissions participants reflected on co-monitoring strategies in case of an emergency. Users described the inter-

Threat Scenarios Tested

Scenario 1: Fire (Physical event in the home)

In this scenario the app systematically notifies users of a house fire (Figure 2) according to homeowner defined access. We ran this scenario two times with each group, first, the homeowner is sent a notification about the threat and is asked to select and discuss their decision to address the threat by choosing an option shown. In the second drill, we instruct the homeowner to not address it. The notification is then sent to others with temporary access if previously granted.

Scenario 2: Cyber (Cyber event in the home)

This scenario presents the user with a notification that there is unusual network activity caused by a device in their home. Options to address the threat are: (1) Shut-down their network, (2) Disconnect the target device (if available), or (3) Declare false alarm.

face as easy to use, but discussed privacy concerns about sharing certain devices, such as a camera, with friends and neighbors. Both groups indicated that they would be especially wary of adding neighbors, however in situations where no one was responding to a potential threat in their home, such as a fire, the participants would certainly want the neighbor to have access.

Task 2. Administrator addressing the threat of fire: A notification of a house fire was presented on the administrators' phone which they were tasked to read and provide a response. In both pilots, the administrator found the alert concerning and opted to call 911, finding this decision to be most appropriate. Users indicated that the response was clear and seeing the image of their home burning motivated them to respond quickly.

Task 3. Threat is addressed by users with temporary access control: In this instance the administrator was told to ignore the notification, emulating a scenario where the administrator is unavailable. After 15 seconds, the notification reaches the next set of respondents, based on permissions. These members were tasked to read and respond to the event in a similar manner as the administrator in the second task. In all cases, co-monitory members alerted 911 of the threat. Furthermore, they stated that the interface was clear, but felt the alert should be paired with a louder noise, flashing graphics, or have the ability to still provide sound if the phone was silenced. Users stated they are willing to forgo levels of privacy and silence in order to preserve the safety of their home or the home of someone they cared for.

Task 4. Addressing a cyber threat: This began similar to task 2 and 3 with the difference being that the notification displayed was related to unusual network or smart-device activity. In this scenario, users indicated that they might shut down the device or network to ensure the concern was addressed, however they felt uncertain about the best approach in this scenario if responding for someone else.

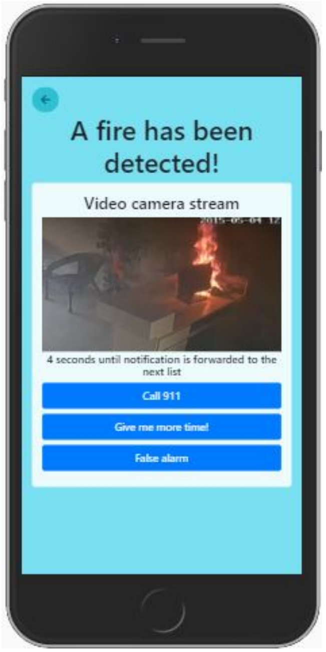
After all tasks had been presented, the groups were asked to envision the application of this access control. This included integration into emergency alert systems and the impacts of various social "roles" that could come under consideration. Users stated they would be very willing to give access to others provided they could not respond to a threat and access was only temporary in nature.

Discussion and Conclusion

The pilot showed that the access control and emergency detection system that smart home users desire is more complex than what is offered by vendors and third party applications that simply allows homeowners a binary option to either share permanent access with others or not. Our initial prototype included various levels of permissions to add individuals by role, but found that considering access based on threat event may provide more context for work on access controls to smart homes.

One of the important layers is a high-level framework of access control policies that allows the owner to define permissions for users, while being flexible enough to provide additional temporary access in case of an emergency situation. We started testing with the Role Based Access Control (RBAC) model, but quickly realized that our implementation required a more dynamic permission management system and modified the RBAC to take into account contextual information derived from the devices. The resulting model is quite different from the original RBAC model, we term this a Role and Event Based Access Control model (REBAC).

Future work should consider an optimized design to implement such a model in an IoT architecture. We will assume a centralized access management system for the purposes



A fire has been detected!

Video camera stream

4 seconds until notification is forwarded to the next list

Figure 2: ThingZone Fire Notification

of our full user study, but a feasible industry implementation needs to be a distributed approach, where each device can employ access controls on its own [1].

Once implemented correctly, this model can be used to greatly improve how emergency situations are detected and addressed that might otherwise cause damage to life and property. Our future research includes expanding user testing and exploring other possibilities like using data analytics and machine learning to study access patterns and detect anomalies, blockchain based security [4], or an IoT centric social network [2].

Acknowledgements

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. Y. Andaloussi, M.D. El Ouadghiri, Y. Maurel, J.M. Bonnin, and H. Chaoui. Access control in iot environments: Feasible scenarios. *Procedia Computer Science*, 130:1031 – 1036, 2018. The 9th International Conference on Ambient Systems, Networks and Technologies (ANT 2018) / The 8th International Conference on Sustainable Energy Information Technology (SEIT-2018) / Affiliated Workshops.

2. Y. Benazzouz, C. Munilla, O. Günalp, M. Gallissot, and L. Gürgen. Sharing user iot devices in the cloud. In *2014 IEEE World Forum on Internet of Things (WF-IoT)*, pages 373–374, March 2014.

3. J. M. Carroll. *Scenario-Based Design*. Indiana University Press, Bloomington, IN, USA, 1995.

4. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram. Blockchain for iot security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 618–623, March 2017.

5. Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. Rethinking access control and authentication for the home internet of things (iot). In *27th USENIX Security Symposium (USENIX Security 18)*, pages 255–272, Baltimore, MD, August 2018. USENIX Association.

6. Statista. IoT: number of connected devices worldwide 2012-2025. `https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/`.

7. Z. Zhang, M. C. Y. Cho, C. Wang, C. Hsu, C. Chen, and S. Shieh. Iot security: Ongoing challenges and research opportunities. In *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, pages 230–234, Nov 2014.

8. K. Zhao and L. Ge. A survey on the internet of things security. In *2013 Ninth International Conference on Computational Intelligence and Security*, pages 663–667, Dec 2013.