Towards a Smart Home Usable Privacy Framework

Chola Chhetri
George Mason University
Fairfax, VA
cchhetri@gmu.edu

ABSTRACT

Smart home devices have gained widespread adoption and are expected to grow rapidly in usage. However, they introduce new challenges to the privacy of the user and the security of the smart society. This paper provides an overview of ongoing dissertation research towards understanding the privacy concerns of smart home device (SHD) users and non-users, a comprehensive analysis of vulnerabilities of SHDs, and the development of smart home usable privacy (SHUP) framework.

INTRODUCTION

I am conducting this research in the Information Sciences and Technology Department of George Mason University. I advanced to candidacy in August 2018 and anticipate completion in May 2021. I am expecting the CSCW doctoral consortium will be an excellent venue to discuss the proposed research with peers, mentors and senior researchers and gain constructive feedback that can be incorporated in this research to enhance its outcomes.

KEYWORDS

Framework; usable privacy; smart home privacy, privacy concerns.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author.
CSCW'19 Companion, November 9–13, 2019, Austin, TX, USA.
© 2019 Copyright is held by the author/owner(s).
ACM ISBN 978-1-4503-6692-2/19/11.
https://doi.org/10.1145/3311957.3361849

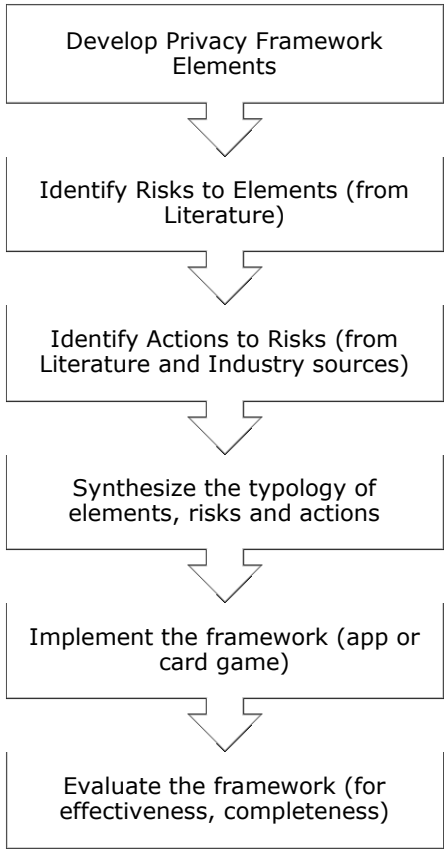

Figure 1: Planned stages for framework development.

CONTEXT AND MOTIVATION

The Internet of Things (IoT) includes non-legacy devices such as coffee makers, refrigerators, thermostats and digital voice assistants that are transforming homes and lives of people. The smart home—a home that includes such Internet-connected IoT devices—provides numerous benefits, such as the convenience of performing household chores, anytime-anywhere control over devices, comfort, safety and security services [6].

However, smart home devices (SHDs) present new challenges to security of the smart home and privacy of its users [5]. Researchers have demonstrated attacks on smart speakers [2], security cameras [2], switches [2], sleep monitors [2], smart locks [7], and application programming frameworks [4]. SHDs collect massive amount of data, which can be used to infer information about users even when traffic is encrypted [3]. SHDs have already been compromised by botnets, such as Mirai, which brought down services like Amazon in 2016 [1]. Such large-scale attacks have a tremendous impact on businesses and society at large.

Despite these problems, market penetration is increasing. One in ten US households contains one smart home device [4]. Nearly half of US adults (46%) reported using digital voice assistants in 2017 [17].

To prevent future smart home disasters and make the smart home a comfortable and trustworthy place for users to live, user concerns must be understood and addressed. It is also essential to explore the vulnerabilities of the smart home, inform the user of safeguards to smart home, and build secure and private smart home solutions.

RELATED WORK

Studies have shown that user understanding of the privacy implications of smart home devices is limited and user mental models of privacy threats are sparse and diverse [15].

Past research has revealed vulnerabilities that impact the privacy of users [2,3,14]. Users appreciate the benefits of smart home devices but worry about violation of their privacy [6]. Users are concerned about extreme data collection [15,16]; however, they need to be reminded, nudged [12], or news-fed [8]. Limited research has been done in understanding privacy concerns of SHD users [11,15], and building tools to help users manage privacy and make informed decisions [13].

Nurse et al. (2016) emphasized the need for a usable framework for modeling smart home security and privacy risks [9]. Although IoT Trust framework of Online Trust Alliance (OTA) provides 16 guidelines on privacy, disclosures and transparency [18], a user-centric framework useful for vendors, developers and users in understanding smart home privacy implications and generating better solutions is essential but lacking.

Table 1: Research Questions

1	What are the security and privacy vulnerabilities of SHDs?
2	What privacy-related concerns do SHD users express?
3	What privacy concerns cause people to not own SHDs?
4	How can we help SHD developers, vendors and users identify smart home risks and take appropriate measures to preserve their privacy?

Table 2: Smart home devices included in the content analysis and sources of user reviews [4]

Devices	Sources
Amazon Echo Dot 2	Amazon.com
Samsung SmartThings Hub	Amazon.com
Google Home	Bestbuy.com
Wink Hub 2	Amazon.com
Insteon Hub	Amazon.com

Table 3: Results of sentiment analysis, temporal analysis, and principle analysis of reviews [4]

User Sentiments	
Negative	74%
Positive	26%
Temporal Concerns	
Data collection	49%
Storage	23%
Sharing	9%
Transmission	2%
Privacy Principles	
Confidentiality	90%
Authentication	10%

RESEARCH APPROACH AND METHODS

This research employs (1) online review analyses, (2) surveys of smart home device users and non-users, (3) cataloging of smart home vulnerabilities from literature, (4) development of a usable privacy framework for smart home devices, with collaborative input on risks and actions from GitHub users, and (5) validation and evaluation of the framework.

PRELIMINARY RESULTS OF REVIEW ANALYSES

Content analysis of online customer reviews of smart home devices was performed to analyze privacy concerns of users (Table 1). Data set for coding and analysis included 128 verified purchase reviews (n=128; Amazon Echo: 120, Google Home: 6, Wink Hub: 1, Insteon Hub: 1) manually extracted with keyword "privacy" and dated from October 2016 to October 2017. Reviews were coded and analyzed [4].

Specific Privacy Concerns

Two-thirds of the users (67%) specified their privacy concern precisely. The top user concern was that these devices were always listening to their conversations. Other major concerns included user tracking, security of private content in cloud, disclosure and discovery of private data [4].

Additional Analyses

Results are summarized in Table 2. User sentiments associated with privacy concerns were mostly negative (74%). The keyword 'concerned' was most often (8/42) used to express user sentiment. Users were mostly concerned about data collection (49%) and confidentiality (90%) [4].

RESEARCH PROJECT STATUS AND NEXT STEPS

Literature review, content analyses, survey questionnaire design, pilot testing, data collection, data analysis, and planning of framework development stages. Next steps include framework development, implementation, evaluation, and dissemination of results.

CURRENT AND EXPECTED CONTRIBUTIONS

This research will help users analyze risks of SHDs and take appropriate privacy preserving steps. It will help researchers, developers and vendors deliver more secure and more private smart home products. It leverages the power of collaborative work in creating risk and action elements of the proposed framework. Table 4 lists six expected contributions from my dissertation research.

Table 4: Expected Research Contributions

1	Insight into privacy concerns of smart home device users
2	Understanding of privacy-related reasons why people refrain from purchasing smart home devices
3	Recommendations for privacy-enhancing smart home solutions
4	Comparison of user and non-user privacy concerns
5	Study of or expansion of privacy paradox (the behavior-attitude gap) in the smart home domain
6	Usable framework for smart home privacy

ACKNOWLEDGMENTS

I thank my advisor Dr. Vivian Motti for advice, support, suggestions, and comments.

REFERENCES

[1] Manos Antonakakis, Tim April, Michael Bailey, et al. 2017. Understanding the Mirai Botnet. Proceedings of the 26th USENIX Security Symposium, 1093–1110.

[2] Noah Apthorpe, Dillon Reisman, and Nick Feamster. 2016. A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic. Data and Algorithmic Transparency Workshop (DAT).

[3] Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster. 2017. Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic. arXiv Preprint.

[4] Chola Chhetri and Vivian Genaro Motti. 2019. Eliciting Privacy Concerns for Smart Home Devices from a User Centered Perspective. Information in Contemporary Society, Springer International Publishing, 91–101.

[5] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. 2016. Security Analysis of Emerging Smart Home Applications. 2016 IEEE Symposium on Security and Privacy (SP), IEEE, 636–654.

[6] Nathaniel Fruchter and Ilaria Liccardi. 2018. Consumer Attitudes Towards Privacy and Security in Home Assistants. Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems, ACM.

[7] Dimitris Geneiatakis, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino, Gary Steri, and Gianmarco Baldini. 2017. Security and Privacy Issues for an IoT based Smart Home. Information and Communication Technology, Electronics and Microelectronics (MIPRO), Croatian Society for Information and Communication Technology, Electronics and Microelectronics - MIPRO, 1292–1297.

[8] Helia Marreiros, Mirco Tonin, Michael Vlassopoulos, and M. C. Schraefel. 2017. "Now that you mention it": A survey experiment on information, inattention and online privacy. Journal of Economic Behavior and Organization 140: 1–17.

[9] Jason R C Nurse, Ahmad Atamli, and Andrew Martin. 2016. Towards a Usable Framework for Modelling Security and Privacy Risks in the Smart Home. Human Aspects of Information Security, Privacy, and Trust. HAS 2016. Lecture Notes in Computer Science, 255–267.

[10] Rodrigo Roman, Pablo Najera, and Javier Lopez. 2011. Securing the Internet of Things. Computer 44, 51–58. Retrieved from doi.ieeecomputersociety.org/10.1109/MC.2011.291.

[11] Deepika Singh, Ismini Psychoula, Johannes Kropf, Sten Hanke, and Andreas Holzinger. 2018. Users' Perceptions and Attitudes Towards Smart Home Technologies. Smart Homes and Health Telematics, Designing a Better Future: Urban Assisted Living, Springer International Publishing, 203–214.

[12] Pamela J. Wisniewski, Bart P. Knijnenburg, and Heather Richter Lipford. 2017. Making privacy personal: Profiling social network users to inform privacy education and nudging. International Journal of Human Computer Studies 98, October: 95–108.

[13] Yaxing Yao. Personalized Privacy Assistant to Protect People's Privacy in Smart Home Environment. Networked Privacy Workshop of the ACM CHI Conference on Human Factors in Computing Systems.

[14] Mengmei Ye, Nan Jiang, Hao Yang, and Qiben Yan. 2017. Security Analysis of Internet-of-Things: A Case Study of August Smart Lock. MobiSec 2017: Security, Privacy, and Digital Forensics of Mobile Systems and Networks, 499–504.

[15] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security & Privacy Concerns with Smart Homes. Symposium on Usable Privacy and Security (SOUPS).

[16] Serena Zheng, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Privacy in Smart Homes. Proceedings of ACM Human-Computer Interaction, 200.

[17] 2017. Nearly half of Americans use digital voice assistants, mostly on their smartphones. Pew Research Center. Retrieved September 24, 2018 from http://www.pewresearch.org/fact-tank/2017/12/12/nearly-half-of-americans-use-digital-voice-assistants-mostly-on-their-smartphones/.

[18] 2017. IoT Security & Privacy Trust Framework v2.5.