The UX of Things: Exploring UX Principles to Inform Security and Privacy Design in the Smart Home

George Chalhoub
Dept. of Computer Science
University of Oxford
george.chalhoub@cs.ox.ac.uk

Abstract
Smart home devices have been successful in fulfilling functional requirements but have often failed at incorporating user-centric security and privacy. This research project addresses the problem of security and privacy in the smart home through the lens of User Experience (UX) Design. Using qualitative interviews with users and designers, we explore the relationship between UX design, security, and privacy in the smart home. This is followed by participatory design workshops with smart home stakeholders to gain an in-depth knowledge of UX design challenges of security and privacy. Our results are further broadened by the development of a conceptual framework for UX design of security and privacy in the smart home.

Author Keywords
User Experience; Internet of Things; Smart Home; Design; Security; Privacy;

CCS Concepts
•**Security and privacy** → **Usability in security and privacy;** •**Human-centered computing** → *Empirical studies in HCI;* User studies;

CHI'20,, April 25–30, 2020, Honolulu, HI, USA
ACM 978-1-4503-6819-3/20/04.
https://doi.org/10.1145/3334480.3381436

User Experience (UX)

The international standard of human-system interaction (ISO 9241-210) defines UX as "*a person's perceptions and responses that result from the use or anticipated use of a product, system or service*".

Research Questions

Main RQ: How can UX design principles be well understood and researched to inform the security and privacy design in the smart home?

RQ1: What is the relationship between UX, security, and privacy in the smart home with regards to (i) users and (ii) design?

RQ2: What are the UX challenges that emerge from designing smart home devices with user-centered security and privacy?

RQ3: How can UX design be incorporated into the design of security and privacy of smart home devices?

Introduction

The rapid increase and growth of IoT (Internet of Things) devices is changing the topography of the internet. IoT devices are expected to generate 90 zettabytes of data and reach market revenue of US$1.1 trillion by 2025 [3]. Despite their growth, IoT devices are raising security and privacy concerns at an unprecedented scale. In 2016, the Mirai botnet infected 600,000 unsecured IoT devices and initiated one of the largest DDoS attacks in history [4]. Moreover, the New York Times' Privacy Project about protecting privacy online recommended people not to use smart home devices unless they are "*willing to give up a little privacy for whatever convenience they provide*" [10]. While there have been efforts to increase security and privacy in smart home devices, the necessity of adopting a user-centered approach has been overlooked. Only a small number of researchers have expressed the need for taking a human-factors approach to the security of smart home devices [2].

Motivation and Background

IoT refers to the billions of physical objects that are connected to the internet, collecting and sharing data. Our research focuses on security and privacy issues in the smart home IoT (e.g., smart speaker, smart thermostat, and smart fridge). There has been controversy over how invasive these technologies are. Users of Amazon Alexa were outraged after a Bloomberg investigation revealed that Amazon contracted thousands of workers to listen to customer audio recordings. An Amazon team in Romania reportedly heard "*private moments including family rows, money and health discussions*" [14]. There have been many calls for IoT manufacturers to take an active role in understanding how their security and privacy solutions align with the UX [13]. UX in IoT is important because UX can fulfill users' needs, ensure positive experiences, and warrant secure and private interactions. UX encompasses a person's emotions, psychological responses, beliefs, perceptions, behaviors, and accomplishments [6].

The UX for IoT devices is different from the UX of conventional digital devices. Unlike common devices such as a laptop or a mobile device, IoT devices typically span across multiple physical and digital interfaces that are interconnected [7]. In addition, the dramatic rise in the number of IoT users and devices significantly increases the complexity of UX design for IoT [5]. Traditional UX design is currently under-equipped to cope with IoT systems and raises numerous challenges such as cross-platform design [15]. IoT devices tend to implement complicated security features and rely on users to learn how to configure and use them [8]. In contrast, IoT privacy tools often prompt users to make a trade-off between convenience and privacy [17].

Problem Statement

Although security and privacy are two of the most researched areas in the smart home, they are barely tackled from a UX point of view. The relationship between UX and the challenge of security and privacy in the context of the smart home is neither well understood nor well researched. Hence, this is an opportunity to research UX design principles and factors in order to build a UX framework for the design of security and privacy in smart home devices.

Preliminary Study

UX Effect on the Security and Privacy of Smart Speaker Users

We conducted a preliminary study to explore the effect of UX on the security and privacy of smart speaker users. Smart speakers (e.g., Google Home, Amazon Echo) dominate the IoT market and were the most popular IoT devices in 2019. Smart speakers are useful and convenient, but they are associated with numerous security and privacy threats because of their always-listening microphones.

Grounded Theory

Grounded Theory is defined as "*the discovery of theory from data systematically obtained from social research*" and is commonly used for conducting qualitative research.

Interview Quotes

Our results establish UX's effect in three areas:

Perception of Risk: "*I make sure I don't say anything risky when it is recording. You know, I'm not going to, like, say my SSN out loud when it's talking.*" (P4)

Experience of harm: "*I really thought the Google Home was innocent and all. Thought the product was great, until I realized that a lot of unintended conversations were recorded, yikes.*" (P8)

Mitigation Practice: "*I just turn it off physically. Not by command or anything. I would just unplug the whole thing. Physically disconnect it. Yeah.*" (P6)

We ran in-depth, semi-structured interviews with thirteen smart speaker users, exploring how and why they use smart speaker technologies, their positive or negative experiences, their security and privacy concerns, and their mitigation or compensatory behavior. Topics that were explored include company trust, always-listening mode, muting speakers, purchasing features and command history.

We recruited the participants (see Table 1) via recruitment flyers, university emails, and local city forum posts. Every participant received a ($12) £10 Amazon gift card voucher for their participation. The sample size (n=13) was determined based on theoretical saturation. We followed a Grounded Theory approach to analyze our data and found six major themes. To validate our findings, we consolidated the existing literature and used meta-synthesis to compare our results with the reviewed literature.

ID	*Age*	*Gender*	*Device(s)*
P1	25-30	F	Google Home
P2	30-35	M	Amazon Echo Dot
P3	35-40	M	Amazon Echo Dot
P4	20-25	M	Google Home Mini
P5	20-25	M	Google Home
P6	20-25	M	Google Home, HomePod
P7	35-40	M	Amazon Echo Dot
P8	20-25	M	Google Home Mini
P9	25-30	M	Amazon Echo Dot
P10	40-45	F	Amazon Echo, Echo Dot
P11	20-25	F	Amazon Echo Dot
P12	25-30	M	Amazon Echo
P13	25-30	M	Amazon Echo

Table 1: Participant Demographics

We found that smart speaker users express lack of privacy concerns towards smart speakers because of certain perceptions (e.g., not being notable, trust, phones have microphones too). The lack of privacy concerns prompts users to trade their privacy for convenience. Despite expressing lack of privacy concerns, various trigger points (e.g., negative experiences, adversarial news) evoke privacy needs. When such needs emerge, existing security and privacy features were found to be hindering the UX of the devices (e.g., muting, using multiple profiles). As a result, users report security and privacy compensatory behavior (e.g., limited use, disconnecting the device, deleting audio history). Six themes were extracted from our analysis (see Table 2).

Perceptions and beliefs towards privacy resignation
Usability of security and privacy controls
Influencers in the privacy and convenience trade-off
Factors affecting smart speaker adoption
Trigger points for security and privacy considerations
Security and privacy compensatory behavior

Table 2: Summary of Our Extracted Themes

Our results show that UX qualities influence security and privacy in three areas: the perception of risk, the experience of harm, and the mitigation practice. Using John Adam's model of risk thermostat [1], we proposed a conceptual model (see Figure 1) demonstrating how UX qualities interact with risk and balancing behavior. In our model, the experience of impact, vulnerability, and threat strongly influence users' perceptions of risk and balancing behavior.

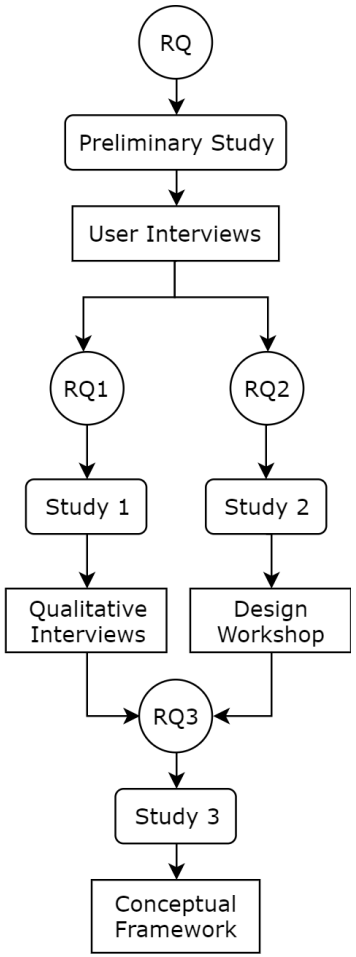

Figure 2: Detailed Research Map

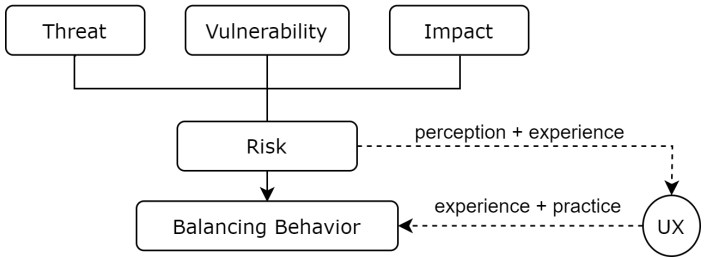

Figure 1: Proposed Conceptual Model

Methodology

The following outlines our research plans (see Figure 2). We will focus on a variety of smart home devices (e.g., smart cameras, doorbells) rather than just smart speakers.

Study One: Exploring user and designer experiences in smart home security and privacy

Interviews with Users: Based on our preliminary results, we know that UX influences security and privacy in: (i) the perception of risk, (ii) the experience of harm and (iii) the mitigation practice. To understand further how UX principles affect those three areas, we are carrying out 13 to 25 semi-structured interviews with smart home users to understand how (i) perceptions in UX influence people's understanding of risk and (ii) how UX influences balancing behavior.

Interviews with Designers: We are also conducting a qualitative investigation with smart home designers aimed to explore (i) how designers take into consideration and evaluate UX in the development of smart home features, (ii) if and how a user-friendly approach is used to develop security and privacy features, and (iii) the challenges faced when designing user-friendly security or privacy solutions. We are conducting around 13 to 25 semi-structured interviews and analyze them based on Grounded Theory.

To further validate our findings, we are planning to conduct quantitative surveys with users and designers to measure how much they align with the findings of our interviews. Also, we aim to parametrize the survey using a vignette study that tackles different design considerations and user scenarios uncovered by the interviews.

Study Two: Exploring UX challenges emerging from smart home security and privacy

Our preliminary study revealed some UX problems found in the security and privacy of smart speakers. This study aims to explore the UX design challenges that arise from designing security and privacy in smart home devices. To achieve this objective, we created participatory design (PD) workshops involving all smart home stakeholders.

Stakeholders were assigned to address a set of problem scenarios (see Table 3) by following a six-step design-thinking activity (see Figure 3). The design activity iterated between problem analysis and framing, creation of potential solutions, and analytical reflection on ideas generated.

Problems	*Scenarios*
Perceptions and Risks	Increase the awareness of the data collection and storage procedures of smart speakers
Security and Usability	Re-design complex or confusing security features and tools of smart locks
Privacy and Control	Design a product that allows users to manage and control their privacy from three smart home products

Table 3: Workshop Scenarios and Problems

Workshop Process

Stakeholders were equipped with a card-based ideation tool for IoT UX, Tiles Ideation Toolkit, which consists of 110 IoT-themed cards grouped in 5 categories: Things, Sensors, Feedback, Human Actions and Services [12]. They were provided with a card-board that scaffolds cards storyboarding and reflection.

The workshop was integrated with user-centered design artifacts (e.g., personas and scenarios) to allow stakeholders to address the security and privacy scenarios [11].

Scoping

The PD workshop is limited to smart home interactions with a focus on the dominant interactions: screen interactions (e.g., Philips HUE, Reality Editor, IFTTT) and speech interactions (e.g., Amazon Echo, Google Home).

The PD workshop incorporated Visser et al.'s model of communicating UX with stakeholders, which consists of three qualities: enhancing empathy, providing inspiration, and supporting engagement [16]. Results would be transcribed and analyzed with Grounded Theory; followed by surveys aimed to parametrize the challenges explored.

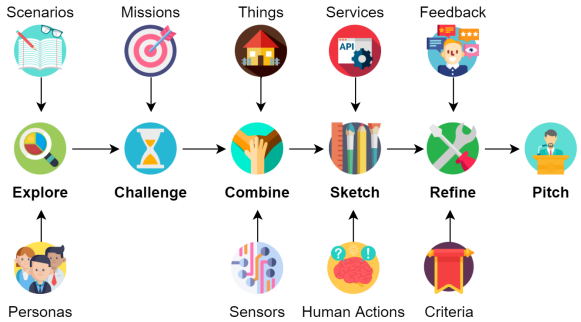

Figure 3: Six-Step Design Workshop Activities

Study Three: Building and evaluating a conceptual framework for UX design

Using the data gathered from previous studies, we aim to build and evaluate a conceptual framework for the UX design of data security and user privacy in smart home devices. This is done via conceptual framework analysis, a literature-based Grounded Theory technique that consists of "*continuous interplay between data collection and data analysis*" [9]. We will follow eight phases (see Figure 4): In Phase 1, we map the selected data sources from early qualitative and quantitative data. This is followed by Phase 2 where we substantially read the selected data and categorize it (e.g., UX factors, security and privacy features). In Phase 3, we examine and re-read the selected data to discover new concepts (e.g., design practices, principles and techniques). In Phase 4, we then deconstruct and categorize the concepts into a table with four columns: concept names, concept description, category, and references. In Phase 5, we integrate and merge similar concepts to reduce redundancy. Phase 6 is a major iterative phase where we synthesize our concepts into a theoretical framework. The phase includes re-synthesis and repetitive synthesis. We seek to evaluate our conceptual frame-work by applying it to a specific design challenge in the smart home (Phase 7). The design challenge would be building a user-centric security and privacy toolkit for smart home devices. We aim to evaluate our toolkit through empirical testing with focus groups (e.g., lab experiment or in-the-wild deployment of an IoT application). In Phase 8, we aim to refine and revise the conceptual framework based on new insights originating from the literature and experimental results.

Contribution and Impact

The results of this proposed research would advance the field of HCI through novel contributions:

- Linking UX design to the security and privacy of smart home devices through qualitative studies with users and designers.
- Investigating the UX challenges encountered during security and privacy design in smart homes.
- Building a conceptual framework for UX design of security and privacy in smart home devices.
- Evaluating the framework with an empirically-tested user-centric security and privacy toolkit for smart home environments.

By bringing UX design to the smart home security and privacy table, we believe that this project will have a significant impact in academia, industry and government organizations. Our framework will form the groundwork of UX design of security and privacy in this emerging technological area.

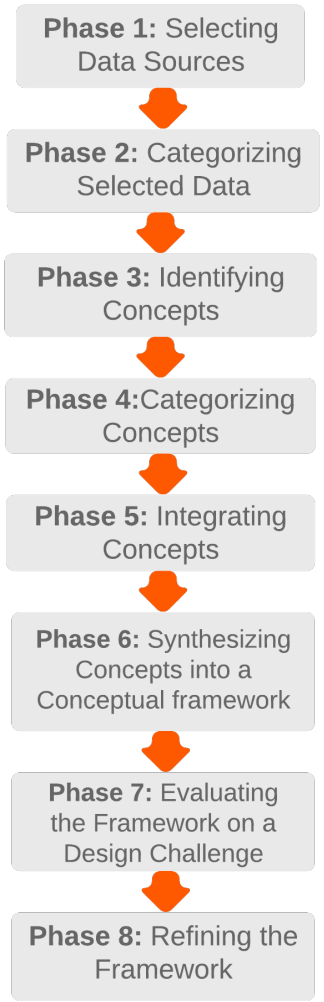

Figure 4: Conceptual Framework Analysis Phases

Acknowledgments

The work is supervised by Prof. Ivan Flechais.

REFERENCES

[1] John Adams. 2003. Risk and morality: three framing devices. *Risk and morality* (2003), 87–106.

[2] Noura Aleisa and Karen Renaud. 2017. Privacy of the Internet of Things: a systematic literature review. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.

[3] Kavi Bains, Mark Giles, Robert Wyrzykowski, and Sylwia Kechiche. 2018. IoT: the $1 trillion revenue opportunity. (May 2018).

[4] Michele De Donno, Nicola Dragoni, Alberto Giaretta, and Angelo Spognardi. 2018. DDoS-capable IoT malwares: Comparative analysis and Mirai investigation. *Security and Communication Networks* 2018 (2018).

[5] Jonathan Follett. 2014. *Designing for emerging technologies: UX for genomics, robotics, and the internet of things*. " O'Reilly Media, Inc.".

[6] Jesse James Garrett. 2010. *The elements of user experience: user-centered design for the web and beyond*. Pearson Education.

[7] Geert de Haan. 2015. HCI Design Methods: where next? from user-centred to creative design and beyond. In *Proceedings of the European Conference on Cognitive Ergonomics 2015*. ACM, 6.

[8] Yong Ho Hwang. 2015. Iot security & privacy: threats and challenges. In *Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security*. ACM, 1–1.

[9] Yosef Jabareen. 2009. Building a Conceptual Framework: Philosophy, Definitions, and Procedure. *International Journal of Qualitative Methods* 8, 4 (Dec. 2009), 49–62.

[10] Thorin Klosowski. 2019. How to Protect Your Digital Privacy. (2019).

[11] Anna Mavroudi, Monica Divitini, Francesco Gianni, Simone Mora, and Dag R. Kvittem. 2018. Designing IoT applications in lower secondary schools. In *2018 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 1120–1126.

[12] Simone Mora, Francesco Gianni, and Monica Divitini. 2017. Tiles: a card-based ideation toolkit for the internet of things. In *Proceedings of the 2017 Conference on Designing Interactive Systems*. ACM, 587–598.

[13] Razvan Nicolescu, Michael Huth, Petar Radanliev, and David De Roure. 2018. State of The Art in IoT-Beyond Economic Value. *London.* (2018).

[14] Nick Parker. 2019. Outrage as Amazon device listens to Brits having sex and swearing. (July 2019).

[15] Claire Rowland, Elizabeth Goodman, Martin Charlier, Ann Light, and Alfred Lui. 2015. *Designing connected products: UX for the consumer Internet of Things*. " O'Reilly Media, Inc.".

[16] Froukje Sleeswijk Visser, Remko Van der Lugt, and Pieter Jan Stappers. 2007. Sharing user experiences in the product innovation process: Participatory design needs participatory communication. *Creativity and innovation management* 16, 1 (2007), 35–45.

[17] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 200.