Factoring User Experience into the Security and Privacy Design of Smart Home Devices: A Case Study

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

Ruba Abu-Salma
Dept. of Computer Science
University College London (UCL)
r.abu-salma@cs.ucl.ac.uk

Ivan Flechais
Dept. of Computer Science
University of Oxford
ivan.flechais@cs.ox.ac.uk

Elie Tom
Dept. of Comp Sci & Engineering
Michigan State University (MSU)
tomelie@msu.edu

Norbert Nthala
Dept. of Media & Information
Michigan State University (MSU)
nthalano@msu.edu

CHI '20 Extended Abstracts, April 25–30, 2020, Honolulu, HI, USA.

ACM ISBN 978-1-4503-6819-3/20/04.
DOI: https://doi.org/10.1145/3334480.3382850

Abstract
Smart home devices are growing in popularity due to their functionality, convenience, and comfort. However, they are raising security and privacy concerns for users who may have very little technical ability. User experience (UX) focuses on improving user interactions, but little work has investigated how companies factor user experience into the security and privacy design of smart home devices as a means of addressing these concerns. To explore this in more detail, we designed and conducted six in-depth interviews with employees of a large smart home company in the United Kingdom (UK). We analyzed the data using Grounded Theory, and found little evidence that UX is a consideration for the security design of these devices. Based on the results of our study, we proposed user-centered design guidelines and recommendations to improve data protection in smart homes.

Author Keywords
User Experience; Smart Home; Design; Security; Privacy; Data Protection.

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

Introduction

The rapidly-growing smart home market is predicted to witness a yearly double-digit growth of 26% [40]. Connected smart home devices, such as smart speakers, thermostats, doorbells, and cameras are found in 134 million households and are expected to reach 234 million households by 2024 [1]. Smart home devices support beneficial features, such as voice-controlled assistants and remote-controlled thermostats, but they also raise new security and privacy risks. A recent report showed that people's concerns about their security and privacy when using smart home devices are increasing, hindering the adoption of these devices [5].

Many efforts have been made to increase security and privacy in the smart home. However, the necessity of adopting a user-centered approach has been overlooked [14]. There have been many calls for Internet of Things (IoT) manufacturers to take an active role in understanding how their security and privacy solutions align with UX [31, 36]. Usability has been an ongoing concern in Human-Computer Interaction (HCI). However, UX encompasses greater considerations such as value, adoptability, and desirability. Yet, these dimensions have not been explored in detail when applied to security and privacy [15]. This seems a missed opportunity to further improve the quality of security and privacy interactions given the UX focus on emotions, psychological responses, beliefs, perceptions, behaviors, and accomplishments [21, 17, 22, 26].

While there is an increased focus on respecting the privacy of smart home users [2, 32, 45, 47, 4, 18], there has been little research into the practices of designers and their collaborators who design these smart home devices [3, 46]. Without an understanding of designers' processes, challenges, and responsibilities, the existing security and privacy issues in these devices will not be easily addressed.

The relationship between UX and the challenge of security and privacy in the context of smart homes is neither well-understood nor well-researched [7, 37]. As a result, we conducted a qualitative investigation with the design team of a smart home company (n=6) to explore how they factored UX into the security and privacy design of their smart camera product. We summarize our findings below:

- We found that the design team did not explicitly factor UX into security design. Some of the reasons were due to being constrained by time, budget, management, and (mis)communication between team members. Designers used their own judgment when thinking about the security aspects of the design process, but no participant took clear responsibility for security design. On the other hand, some UX aspects of privacy were considered by the design team, due to complying with regulatory obligations (e.g., GDPR).
- We uncovered different UX design challenges that were associated with the security and privacy of smart homes. Based on the study results, we extracted a set of design recommendations to improve data protection in smart homes.

Related Work

The current literature suggests that security and privacy may pose UX challenges for IoT stakeholders. Oh and Lee [33] analyzed reviews of quantified self applications and found that privacy was a key problem affecting both UX and security and privacy design processes. This was later confirmed by Bergman et al. [8], where they explored how 11 IoT companies captured UX requirements and found that security and privacy posed a UX challenge for designers. Rowland et al. [37] found that four factors affected UX in the design of IoT products: socio-cultural, ecological, behavioral, and operational factors.

	Research Questions
RQ1	What are the stakeholder practices when designing smart home devices?
RQ2	Do designers follow a UX approach when designing and improving the security and privacy of smart home devices?
RQ3	What are the UX challenges that stakeholders face when designing for security and privacy?

Table 1: Research Questions

	Job	Age
P1	Product Manager	46
P2	UX Designer	28
P3	Information Security Officer	42
P4	Security Engineer	30
P5	Hardware Designer	32
P6	UX Director	44

Table 2: Participant Demographics

Some UX frameworks and models have been built to assist designers. For example, Lin et al. [24] developed a data-driven framework, UNISON, which captures UX during the IoT development process. Similarly, Olsson et al. [34] developed and empirically evaluated UDIT (User Dimension In IoT), a model which identifies user interactions with IoT interfaces and ecosystems.

Methodology

To address our research questions (see Table 1), we devised an exploratory qualitative study based on approaches described in prior work [27, 28, 9] and focused on the specific case of a company designing smart home products. Case study research is a detailed inquiry of an issue used to evaluate the authenticity of the issue, and allows researchers to gather realistic data of the phenomenon being investigated in social and behavioral scientific research [44].

Recruitment

We conducted our case study with six participants. We recruited two participants on LinkedIn, a professional networking service. We recruited the remaining four participants through snowball sampling [19]. This allowed us to reach employees that were not easily accessible through other sampling strategies. At the time of recruitment, the employees were active at the company and responsible for the design or maintenance of a smart home product.

Interview Procedure

We conducted semi-structured interviews with six employees of a smart home company (see Table 2) that manufactured a wide range of smart devices. We asked participants to complete a short survey to gather some demographic information (e.g., age, gender, job title and description) before proceeding to the interview. We used the funnel technique [13] to structure our interview questionnaire (study script), starting with general questions and then drilling down to specific ones. We first asked general questions about participants' work experience and employment at the company (e.g., responsibilities, duration of employment). We then asked questions revolving around the type of smart home devices that the company manufactured. We then asked specific questions about the development lifecycle of their smart security camera (e.g., design, development, deployment, maintenance). In addition, we explored how UX practices, requirements gathering, and testing were addressed during the design phase (e.g., prototyping, qualitative and quantitative research methods used). Lastly, we asked participants to discuss how security and privacy were factored into the design phase. We conducted the interviews remotely using Skype and Zoom. We audio-recorded and transcribed the six interviews. Interviews lasted for an average of 46 minutes.

Pilot Study

After designing our initial interview questions, we conducted a small-scale pilot study with four designers of smart home devices at a local IoT security conference[1]. Two researchers recorded, transcribed, and analyzed the pilot interviews. We used the findings to identify potential problems (e.g., adverse events, time and cost) in advance prior to conducting the full-scale study.

Data Analysis

We analyzed the interview transcripts using Grounded Theory following Strauss and Corbin's procedure [39]. One researcher conducted the six interviews, and then two researchers (including the interviewer) analyzed the transcripts independently. The researchers met frequently to

[1] We conducted our pilot study at the third Annual Secure Internet of Things Security Conference in November 2019 in Reading, UK.

Requirements	Example
Functionality	Integration with a smart assistant
Usability	Ability to set-up the camera without difficulties
Security	Encryption between device and mobile application
Privacy	Adding a privacy mode in the mobile application
Compliance with the Law	Compliance with GDPR regulations

Table 3: Different Requirements Communicated Among Stakeholders

Practices	Example
Non-use of Encryption	Sending sensitive data unencrypted
End-user Incompetence	Falling for phishing attacks

Table 4: Insecure Cyber Practices Identified by Stakeholders

compare, review, and merge their categories. They resolved all disagreements and identified 140 codes in total.

Research Ethics

Oxford University's Central University Research Ethics Committee (CUREC) reviewed and approved our research study. At the beginning of each interview session, we gave each participant an information sheet and a consent form which they had to sign before taking part in our study.

Results

We conducted our study with a large smart home company that contracted more than 500 employees and had more than 2 million customers. The company sold a wide range of smart home devices, such as security cameras, smart thermostats, and smart lights. We focused on the design, development, and implementation of a flagship security camera product that had been in production for years. We chose this product because smart home security cameras (i) have a growing adoption rate [30] and (ii) are subject to increased security attacks [10].

Design and Development Process

A cross-functional team that involved various stakeholders (e.g., senior UX designers, UI designers, software developers, mobile developers, industrial designers, product managers) was in charge of exploring and making decisions. The team ran multiple workshops and followed a collaborative design process (multi-staged UX [23]). The team combined hardware and software development in agile [25] and iterative [11] design processes. We identified five types of requirements that stakeholders negotiated during the early stages of projects: functionality, usability, security, privacy, and legal requirements (see Table 3).

Privacy and Trust

Five participants mentioned that consumer trust was crucial for the adoption and use of their products. Trust was considered part of the success strategy and was described as *"extremely important for users buying physical security products"* (P1). The company maintained trust by making efforts to prevent insecure cyber practices, such as developers' non-use of encryption and end-user incompetence (see Table 4). The company also adopted an incident response plan in case of a breach, in order to maintain its reputation, which we identified as a potent motivator for privacy considerations in the design phase. In order to maintain trust, designers considered some UX factors affecting privacy (e.g., privacy UX [29]). The goal of UX designers was to make sure users felt comfortable with the camera, and that it did not make users feel it was a *"tool of surveillance"* (P6). To achieve this goal, UX Designer P2 interviewed psychologists and visited existing customers to identify acceptable and non-intrusive *"areas of monitoring"* (see Figure 1). Designers also aimed to make users *"feel in control"* by adding a visible on/off state of the camera as well as a privacy mode in the mobile application to give users *"peace of mind"* (P2). The privacy mode allowed users to disable the camera using their mobile application.

Security Culture

We asked our participants about security design to investigate how it was factored into the design phase of the camera product. We found that the *Information Security Team* was not involved in the design phase of the product. They stated that all designers had to follow the company's *"information security management framework"* (P3). Five participants mentioned that security was viewed mostly as a technical problem. For example, Product Manager P1 did not *"see the value"* of including security experts in the design team, and chose security features – such as authen-

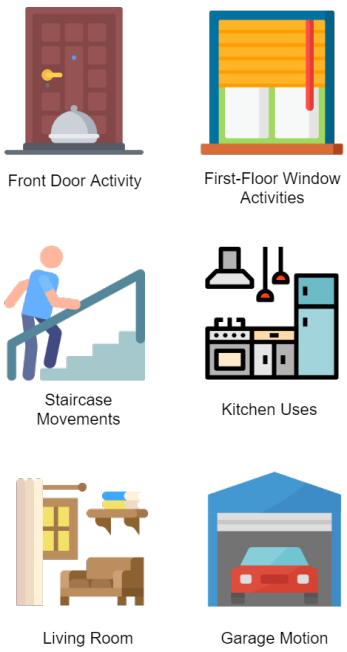

Figure 1: While conducting UX research, P2 visited existing clients in their house to explore acceptable areas of monitoring.

tication – based on their understanding of common security practices. However, P1 said the *Information Security Team* bore the responsibility for all matters related to security, including security design. Even though security was considered as an afterthought, we found that legal liabilities (e.g., GDPR [41]) required companies to encompass *"Data Protection by Design"* [12] practices (P3). The company's *Legal Counsel Department* pushed security and privacy requirements during the early design phase through data protection officers. The officers were not part of the cross-functional team and communicated the requirements through emails. Product Manager P1 expressed frustration over email communication and described data protection officers as acting *"from a point of authority."*

Design Challenges

We uncovered design challenges that participants faced in the context of UX and security and privacy design. Project constraints (e.g., time, budget) were claimed to influence the security design: P3 revealed that the *Information Security Team* was allocated 10% of the total budget of the project, which was believed to be *"not enough,"* and described adding security experts to the design team as a *"luxury"* they could not afford. UX Director P6 said they were *"time-pressured"* and could not conduct the user research required to understand security behavior. Moreover, the agile development of hardware and software systems created a design challenge for industrial designers because adding security features to a physical camera was not easy. Hardware Designer P5 said *"while mobile developers are flexible, we have to make early decisions that are not easy to change."* Moreover, third-party services such as Amazon's smart intelligent assistant Alexa *"improve the experience"* of users (P2); however, they created difficulties for security stakeholders. Security Engineer P4 – who worked on encrypting the data transferred between the company's ecosystem of products and Amazon Alexa – described the process as *"complex"* and "time-consuming." Lastly, UX Director P6 expressed concerns over the lack of standards that regulated UX design in the smart home. P6 also indicated that regulatory requirements such as GDPR complicated the design process due to being *"basic"* and *"vague."*

Discussion

Our findings support the existence of a long-term challenge in IoT systems where security is treated as a technical problem (e.g., [43]), regardless of ongoing efforts to bridge social and technical aspects of security design [48]. We argue that this can contribute to the growing semantic attacks on end-users of IoT devices (e.g., the December 2019 attack on the Ring smart camera where an attacker managed to compromise a family's user account and gained control of the camera [42]). In addition, evidence emphasizes the need for considering UX in the design of security features of systems. The study by Shava and Greunen [38] found that 40% of respondents easily entrusted anyone who claimed to be part of a technical support team — a potential for falling for a phishing attack. Without the involvement of security experts in the design team and with an absence of user engagement in security during the design process, issues which can impact the design of security features (e.g., the need for secure authentication mechanisms such as two-factor authentication which can mitigate phishing attacks) cannot be anticipated.

Our results also give an example of a common communication problem in multi-stakeholder teams where security design happens. As Flechais and Sasse [16] report, in the absence of day-to-day communication between stakeholders, the number of implicit assumptions made increases (e.g., in our study, the product manager selecting security features based on their knowledge of common practices). The in-

Acknowledgments

This research is supported by a 2018-2019 research grant from the Information Commissioner's Office (ICO).

troduction of legal requirements (e.g., GDPR) that traverse the design phase makes the problem more complex. This was shown in our study where UX Director P6 faced difficulties dealing with the vagueness of GDPR's data protection guidelines. While GDPR requires data protection by design, it can bring more confusion to the design table: regulatory requirements have been reported to be high-level and impractical [20], and their implementation requires new techniques and tools. In addition, expecting largely autonomous groups of stakeholders (e.g., security, legal, design, UX) with different goals, motivations, and constraints to speak the same language and implement required controls is simply impossible. The larger the number of stakeholders, the more assumptions will be made.

Recommendations

Based on our case study findings, we put forward the following design recommendations intended to address some of the challenges that designers face.

- **Design teams should be diversified to include all domains:** Our results show that design teams lack security expertise (c.f., Results/Security Culture). UX is not only a designer's problem. Barnum [35] found that UX professionals come from many diverse backgrounds. All stakeholders (including security experts, designers, and legal experts) influence the UX of a product.
- **Educate and motivate design teams about UX in security and privacy:** As Flechais and Sasse [16] discuss, education and motivation are important to counter communication breakdown within multi-stakeholder design teams (c.f., Results/Security Culture), and that it is crucially important to clarify each stakeholder's responsibilities and how stakeholders can achieve their goals.
- **Address the UX of hardware products:** We usually think of UX in the context of software. However, UX is crucial for the development of user-centered hardware products, especially smart home products that increasingly need to present pleasing design aesthetics and intuitive affordances (c.f., Results/Design Challenges). For example, Zheng et al. [47] stated that most smart home devices do not have screens and recommended the addition of user-friendly visual indicators that do not overwhelm users.
- **Develop innovative solutions to comply with GDPR:** The introduction of GDPR regulations brings challenges to smart home designers (c.f., Results/Design Challenges) and is likely to require innovative solutions. Bastos et al. [6] also suggest that other design challenges accompany GDPR. Product teams should invest in novel design tools and innovative solutions that aim to address these challenges.

Conclusion and Future Work

We conducted a case study with six employees who played a role in the design of a smart camera. We presented preliminary evidence that designers of smart home devices do not explicitly or systematically consider UX in designing security features. We also reported several factors which are at the root of design challenges – some of which have been reported in the broad domain of security. We argue that more work needs to be done to explore more widely how UX is considered in security design and what further challenges exist in this area, if cyberattacks targeting smart homes are to be contained. Further research would be required in order to have a better understanding of the design process, such that stakeholders with the best capabilities can better address the challenges of UX in the context of security, privacy, and data protection.

REFERENCES

[1] Statista . 2020. Smart Home - worldwide | Statista Market Forecast. (Jan. 2020). https://www.statista.com/outlook/279/100/smart-home/worldwide

[2] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*.

[3] 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*.

[4] Noah Apthorpe, Dillon Reisman, and Nick Feamster. 2017. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *arXiv preprint arXiv:1705.06805* (2017).

[5] Parks Associates. 2019. Parks Associates: Privacy concerns increasing among smart home device owners. (Oct. 2019).

[6] Daniel Bastos, Fabio Giubilo, Mark Shackleton, and Fadi El-Moussa. 2018. GDPR Privacy Implications for the Internet of Things.

[7] Johanna Bergman and Isabelle Johansson. 2017. The user experience perspective of Internet of Things development. (2017).

[8] Johanna Bergman, Thomas Olsson, Isabelle Johansson, and Kirsten Rassmus-Gröhn. 2018. An exploratory study on how Internet of Things developing companies handle User Experience Requirements. In *International Working Conference on Requirements Engineering: Foundation for Software Quality*. Springer, 20–36.

[9] Dennis Basil Bromley and Dennis Basil Bromley. 1986. *The case-study method in psychology and related disciplines*. Wiley Chichester.

[10] Matt Burgess. 2018. The IoT's security nightmare will never end. You can now search insecure cameras by address. *Wired UK* (Nov. 2018). https://www.wired.co.uk/article/internet-of-things-security-camera-search-location

[11] William Buxton and Richard Sniderman. 1980. Iteration in the design of the human-computer interface. In *proceedings of the 13th Annual Meeting of the Human Factors Association of Canada*, Vol. 7281. 37.

[12] Lee A. Bygrave. 2017. Data protection by design and by default: Deciphering the EU's legislative requirements. *Oslo Law Review* 4, 02 (2017), 105–120.

[13] Charles F. Cannell, Peter V. Miller, and Lois Oksenberg. 1981. Research on interviewing techniques. *Sociological methodology* 12 (1981), 389–437.

[14] Isis Chong, Aiping Xiong, and Robert W. Proctor. 2019. Human factors in the privacy and security of the internet of things. *Ergonomics in Design* 27, 3 (2019), 5–10.

[15] Paul Dunphy, John Vines, Lizzie Coles-Kemp, Rachel Clarke, Vasilis Vlachokyriakos, Peter Wright, John McCarthy, and Patrick Olivier. 2014. Understanding the experience-centeredness of privacy and security technologies. In *Proceedings of the 2014 New Security Paradigms Workshop*. ACM, 83–94.

[16] Ivan Flechais, M. Angela Sasse, and Stephen Hailes. 2003. Bringing security home: a process for developing secure and usable systems. In *Proceedings of the 2003 workshop on New security paradigms*. ACM, 49–57.

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

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

[19] Leo A. Goodman. 1961. Snowball sampling. *The annals of mathematical statistics* (1961), 148–170.

[20] Seda Gürses, Carmela Troncoso, and Claudia Diaz. 2015. Engineering privacy by design reloaded. In *Amsterdam Privacy Conference*. 1–21.

[21] Marc Hassenzahl, Sarah Diefenbach, and Anja Göritz. 2010. Needs, affect, and interactive products–Facets of user experience. *Interacting with computers* 22, 5 (2010), 353–362.

[22] Marc Hassenzahl and Noam Tractinsky. 2006. User experience-a research agenda. *Behaviour & information technology* 25, 2 (2006), 91–97.

[23] Lassi A. Liikkanen, Harri Kilpiö, Lauri Svan, and Miko Hiltunen. 2014. Lean UX: the next generation of user-centered agile development?. In *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational*. ACM, 1095–1100.

[24] Kuo-Yi Lin, Chen-Fu Chien, and Rhoann Kerh. 2016. UNISON framework of data-driven innovation for extracting user experience of product design of wearable devices. *Computers & Industrial Engineering* 99 (2016), 487–502.

[25] Robert C. Martin. 2002. *Agile software development: principles, patterns, and practices*. Prentice Hall.

[26] John McCarthy and Peter Wright. 2007. *Technology as experience*. MIT press.

[27] Sharan B. Merriam. 1988. *Case study research in education: A qualitative approach.* Jossey-Bass.

[28] Sharan B. Merriam. 1998. *Qualitative Research and Case Study Applications in Education. Revised and Expanded from" Case Study Research in Education.".* ERIC.

[29] Gabe Morazan. 2019. What Is Privacy UX? (May 2019). `https://www.cmswire.com/digital-experience/what-is-privacy-ux/`

[30] Jack Narcotta. 2018. Smart Home Surveillance Camera Market Analysis and Forecast. (April 2018).

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

[32] Norbert Nthala and Ivan Flechais. 2018. Informal support networks: an investigation into home data security practices. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 63–82.

[33] Jeungmin Oh and Uichin Lee. 2015. Exploring UX issues in Quantified Self technologies. In *2015 Eighth International Conference on Mobile Computing and Ubiquitous Networking (ICMU)*. 53–59. `DOI: http://dx.doi.org/10.1109/ICMU.2015.7061028`

[34] Helena Holmström Olsson, Jan Bosch, and Brian Katumba. 2016. User Dimensions in 'Internet of Things' Systems: The UDIT Model. In *Software Business (Lecture Notes in Business Information Processing)*, Andrey Maglyas and Anna-Lena Lamprecht (Eds.). Springer International Publishing, Cham, 161–168. DOI: http://dx.doi.org/10.1007/978-3-319-40515-5_13

[35] Janice Redish and Carol Barnum. 2011. Overlap, influence, intertwining: The interplay of UX and technical communication. *Journal of Usability Studies* 6, 3 (2011), 90–101.

[36] Claire Rowland and Martin Charlier. 2015. *User Experience Design for the Internet of Things*. O'Reilly Media.

[37] 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.".

[38] F. B. Shava and D. Van Greunen. 2013. Factors affecting user experience with security features: A case study of an academic institution in Namibia. In *2013 Information Security for South Africa*. 1–8. DOI: http://dx.doi.org/10.1109/ISSA.2013.6641061

[39] Anselm Strauss and Juliet M. Corbin. 1997. *Grounded theory in practice*. Sage.

[40] Jitesh Ubrani, Ramon Llamas, and Michael Shirer. 2019. Double-Digit Growth Expected in the Smart Home Market, Says IDC. (March 2019). https://www.idc.com/getdoc.jsp?containerId=prUS44971219

[41] Paul Voigt and Axel Von dem Bussche. 2017. The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing* (2017).

[42] Elizabeth Wolfe and Brian Ries. 2019. Ring camera: A hacker accessed a family's security camera told their 8-year-old daughter he was Santa Claus - CNN. (Dec. 2019). https://edition.cnn.com/2019/12/12/tech/ring-security-camera-hacker-harassed-girl-trnd/index.html

[43] Teng Xu, James B. Wendt, and Miodrag Potkonjak. 2014. Security of IoT systems: Design challenges and opportunities. In *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design*. IEEE Press, 417–423.

[44] Robert K. Yin. 2017. *Case study research and applications: Design and methods*. Sage publications.

[45] Eric Zeng and Franziska Roesner. 2019. 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)*. 159–176.

[46] Kai Zhao and Lina Ge. 2013. A survey on the internet of things security. In *2013 Ninth international conference on computational intelligence and security*. IEEE, 663–667.

[47] 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.

[48] Mary Ellen Zurko. 2005. User-centered security: Stepping up to the grand challenge. In *21st Annual Computer Security Applications Conference (ACSAC'05)*. IEEE, 14–pp.