A USER-CENTERED APPROACH TO DIGITAL HOUSEHOLD RISK MANAGEMENT

Cristina Paupini[1] [0000-0003-4139-6331] G. Anthony Giannoumis[1] [0000-0001-7939-6340] Terje Gjøsæter[1] [0000-0002-1688-7377]

[1] Oslo Metropolitan University, 0130 Oslo, Norway
cristina.paupini@oslomet.no

Abstract.
Internet of Things (IoT) is expected to become as common as electricity (OECD 2016) and there is a high probability for connected homes to become central parts of critical societal. IoT technologies might access, manage and record sensitive data about citizens and, as they become more and more pervasive, unintended data breaches reports increase every week. However, most of the tools designed to protect users' privacy and personal data on IoT devices fail to contemplate the experience of persons with disabilities, elderly and other vulnerable categories of people. As a consequence, they are forced to rely on the help of family members or other related persons with technical skills, as frequent technical problems turn out to be the rule rather than the exception. With humans traditionally considered to be the "weak link" in technological networks there is the need of a vast educational project to raise awareness on the subject. This ongoing research paper aims to fill the existing gap in research by asking how humans deal with the risk factors linked to connected homes and how to develop a universally designed set of tools for everyday risk management in connected homes.

Keywords: Universal Design, Internet of Things, Connected Homes.

1 Introduction

Home has always been a focal point of society's activities and decision - making, providing shelter and security to its inhabitants [1]. Recent technological innovations continue to change society through widespread and broadly accessible internet, artificial intelligence and machine learning [2]. Internet of Things (IoT), here referred to as the interconnection via the Internet of computing devices embedded in everyday objects, allowing their management, data mining and the access to the data generated [3], is expected to become as common as electricity (OECD 2016). There is therefore a high probability for connected homes to become central parts of critical societal infrastructures [1]. As a consequence, it is necessary to address the digital risks and vulnerabilities that come with the development of IoT consumer products and services. Privacy and security have emerged as two critical areas of risk when it comes to accessing and using technology [4]. This is especially relevant for IoT technologies as they access, manage and record sensitive data about people. As they become more and more pervasive, unintended data breaches reports increase every week [5].

However, most of the tools designed to protect users' privacy and personal data on IoT devices are not accessible for persons with disabilities, older persons and other groups of socially disadvantaged people [6]. As a consequence, they are forced to rely on the help of family members or other related figures with technical skills [7]. With humans traditionally considered to be the "weak link" in technological networks [8], there is the need for more evidence and awareness on the relationship between privacy and accessibility concerning IoT technologies. This paper presents the ongoing research that aims to fill this gap asking the following research question: how do the perceived risks linked to connected households and homes differ from the actual risks IoT comes with and how do humans deal with those risk factors?

2 State of the Art

2.1 Internet and Communication Technology and Internet of Things

The fourth industrial revolution is bringing a drastic change of paradigm in our society by introducing widespread and broadly accessible internet, smaller, cheaper and more powerful sensors, artificial intelligence and machine learning [2]. Technology is being more and more intertwined with the very fabric of our society [9], and the more people become connected, the more they tend to inhabit connected homes. The environment itself is becoming widely connected through smart cities and vehicles, affecting industries and the public sector as well as individuals [10]. Traditional physical and societal infrastructures connecting homes to key services are currently being digitalized. According to IEC (2015), 200 million Internet connected wireless smart home security and safety products will have been installed worldwide by 2020. Scholars' interest has been drawn to explore IoT's characteristics in an numerous research works, from the pure definitions of Internet of Things and the early stages of its application [4] [11] [12] to the effects of its implementation and whether or not Europe is (was) ready for it [2]. Furthermore, several studies explore IoT possible adaptation in smart cities and environments, households and services [11], [12].

2.2 The risks connected to Internet of Things

While information technology benefits society in numerous ways, it also has potential to create new vulnerabilities, even while attempting to solve other problems [13]. With this in mind, our reliance on digital infrastructures implies that digital risks and vulnerabilities must be addressed, managed and reduced. Internet of Things, in particular, is the setting stone of the futuristic imaginary of a day-to-day reality where objects come alive and actively upgrade our routine [14]. It is therefore crucial to note that IoT devices, especially home-based ones, often come with a deficiency in proper security systems and upgrade opportunities [15]. In his dissertation, Angrishi argues that these smart devices should be considered as computers that "do specialized jobs",

rather than as specialized devices with built-in intelligence. What really differentiates IoT devices from computers is that their design often does not include security at all [14]. Hewlett-Packard (HP) in 2014 released a study about the most popular devices in some of the most common IoT niches at the time, reporting an average of 25 vulnerabilities per device. According to the study, "80% of devices failed to require passwords of sufficient complexity and length, 70% did not encrypt local and remote traffic communications, and 60% contained vulnerable user interfaces and/or vulnerable firmware" [16]. Some of the reasons for this exposure may be found in their lack of well-defined perimeters, their highly dynamic and mobile nature and heterogeneity in respect to communication medium and protocols [17]. To sum up, most studies indicate privacy and security are the two main areas of risk individuated for digital households, but few have investigated those risks for vulnerable categories such as people with disabilities and older persons.

2.3 Human relation with privacy and data security

In addition to Internet of Things devices' default criticalities regarding privacy and security, numerous scholars focused on people's approach to data protection and privacy. Users are in fact traditionally considered to be the weak spot in technological networks [8], a belief that is frequently linked to the so called "privacy paradox"[18], also known as humans' tendency towards privacy-compromising behavior online eventually resulting in a dichotomy between privacy attitudes and actual behavior [19]. This conduct seems to characterize even privacy conscious individuals that, especially online, do not live up to their declared privacy preferences [20]. However, as observed by Acquisti and Grossklags in 2005, "individuals make privacy-sensitive decisions based on multiple factors, including (but not limited to) what they know, how much they care, and how costly and effective they believe their actions can be.", meaning that the dichotomy between stated and implemented preferences does not inevitably imply the existence of the paradox [21]. Furthermore, even when the purpose to reduce data disclosure is present, due to the unfamiliarity of the average person the actual disclosure considerably exceeds intention [18] [22]. The majority of research into the privacy paradox and users' attitude towards privacy and data security focuses on e-commerce and social networking [18] and there is a noticeable general tendency to not consider vulnerable categories of people, such as the ageing population and persons with disabilities, as particularly exposed to risks in digital environments.

2.4 Universal Design

According to the United Nations Convention on the rights of Persons with Disabilities (CRPD), "Universal design means the design of products, environments, programs and services to be usable by all people, to the greatest extent possible, without the need for adaptation or specialized design. (art.2). As shown in the previous sections, there are many studies of privacy and security in relation to IoT devices, but most of them fail to consider the experience of people with disabilities [6]. It is striking to

notice how most of the tools implemented for security and privacy protection, for instance, rely on subtle visual cues or other potentially inaccessible indicators. Constant interaction with such reality might cause extreme frustration or total inability to users with perceptual limitations [6]. Due to the limitations in the design of IoT devices, including products for connected households, persons with disabilities are often dependent on the help of family members. Frequent technical problems appear to be the rule rather than the exception [7]. Acknowledging these situations means acknowledging the need for a change in the way we approach security and privacy risk factors in IoT environments and devices towards a more inclusive perspective.

3 Methods

In order to answer the research question above, a transdisciplinary and interdisciplinary approach was adopted. The projects on which this paper is based is a collaboration between the Sociology and Computer Science departments and the researchers involved come from a variety of different fields. From Universal Design to ICT and Social Media to Education and Sociology, elements from the different disciplines were brought in to contribute to the outline and realization of the research.

The project involves a group of twenty households selected with varying social and demographic characteristics. The participants are directly involved in various steps of the research. Multiple research methods from different fields were adopted during the research, including in-depth interviews, participant observation, multimedia documentary data, and a survey. First, a set of semi-structured interviews were carried out in the participants' homes. This method allowed informants the freedom to express their views in their own terms while providing reliable, comparable qualitative data [23]. The participants also drew a floor map of their house and indicated where each IoT device was typically placed. Pictures of the devices were collected as additional documentation. Second, a house visit and follow-up interviews were conducted and the participants were asked to reenact their typical home routines in order to illustrate their use of IoT devices.

Following each house visit, a risk assessment of the IoT devices in the home was performed using a Risk Assessment Model, which was developed as part of the research project. The assessment consists of 15 questions that examine different characteristics of the IoT device. The assessment is divided into five sections that evaluate 1) the device's connectivity and protocols used to connect to public and private networks, 2) data transmission and encryption, 3) user authentication, 4) the Operating System's update procedures, and 5) data storage, data protection guarantees and end user license, guide and procedures. The questionnaire ends with a subjective open question that aims to assess on a scale from 1 to 5 the negative impact that a malfunction or a data breach in the analyzed device would have over the house and its owner. A thematic analysis of documentation from the home visits and interview

transcripts is to be conducted in order to disclose the perceived risks among the users and their families. These themes are meant to be compared to the results of the risk assessment in order to highlight any difference.

4 Preliminary Results and Discussion

Due to the rampant global coronavirus pandemic, the research was forced to a suspension. However, a first pilot study has been conducted and the preliminary data is being analyzed. The pilot allowed the methods to be tested and their efficacy to be confirmed by the quantity and quality of data gained in various forms. However, it is possible that the present conditions, if prolonged in time, will require a change in the approach to the methods and the whole research.

5 Conclusions and Future work

With Internet of Things (IoT) expected to be as common as electricity (OECD 2016) there is a high probability for connected homes to become central parts of critical societal. It is therefore crucial to note that IoT devices, especially home-based ones, often come with a deficiency in proper security systems and upgrade opportunities [15]. This issue is particularly evident when addressing the experience of persons with disabilities, elderly and other vulnerable categories of people, which most tools for privacy protection fail to contemplate. With humans traditionally considered to be the "weak link" in technological networks there is the need of a vast educational project to raise awareness on the subject.

The next steps in the research include the creation of a set of tools for households IoT risk management, which will be developed in collaboration with stakeholders and designers. The intention is to emphasize the active involvement of research participants throughout the research, as co-researchers [24]. The framework adopted comes from the Participatory Action Research, as "the way groups of people can organize the conditions under which they can learn from their own experiences and make this experience available to others" [25]. In this project, action research is to be integrated by a combination of techniques from Co-design and Participatory Design. Co-design here is intended as collective creativity applied across the whole span of a design process [26], whether Participatory Design is considered as a process of investigating and supporting mutual learning between multiple participants [27].

6 Acknowledgements

The research this paper is based on is part of the *RELINK - Relinking the "weak link". Building resilient digital households through interdisciplinary and multilevel exploration and intervention* project. The research project is funded by the Research

Council of Norway, IKTPluss, grant no. 288663, and is headed by Consumption Research Norway (SIFO) and Oslo Metropolitan University (OsloMet).

7 References

1. Helle-Valle, J. and D. Slettemeås, *ICTs, domestication and language-games: a Wittgensteinian approach to media uses.* New media & society, 2008. **10**(1): p. 45-66.
2. Kuruczleki, E., et al., The Readiness of the European Union to Embrace the Fourth Industrial Revolution. Management (18544223), 2016. **11**(4).
3. Dorsemaine, B., et al. Internet of things: a definition & taxonomy. in 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies. 2015. IEEE.
4. Atzori, L., A. Iera, and G. Morabito, *The internet of things: A survey.* Computer networks, 2010. **54**(15): p. 2787-2805.
5. Ferrara, P. and F. Spoto. *Static Analysis for GDPR Compliance*. in *ITASEC*. 2018.
6. Sauer, G., et al., *Accessible privacy and security: a universally usable human-interaction proof tool.* Universal Access in the Information Society, 2010. **9**(3): p. 239-248.
7. Fuglerud, K.S. The barriers to and benefits of use of ICT for people with visual impairment. in International Conference on Universal Access in Human-Computer Interaction. 2011. Springer.
8. Sasse, M.A., S. Brostoff, and D. Weirich, Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. BT technology journal, 2001. **19**(3): p. 122-131.
9. Schwab, K., *The fourth industrial revolution*. 2017: Currency.
10. Vulkanovski, A., Home, Tweet Home": Implications of the Connected Home, Human and Habitat on Australian Consumers. Sydney: Australian Communications Consumer Action Network, 2016.
11. Bertino, E. Data Security and Privacy in the IoT. in EDBT. 2016.
12. Zanella, A., et al., *Internet of things for smart cities.* IEEE Internet of Things journal, 2014. **1**(1): p. 22-32.
13. Ransbotham, S., et al., *Special section introduction—ubiquitous IT and digital vulnerabilities.* Information Systems Research, 2016. **27**(4): p. 834-847.
14. Angrishi, K., Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets. arXiv preprint arXiv:1702.03681, 2017.
15. Xi, W. and L. Ling. Research on IoT privacy security risks. in 2016 International Conference on Industrial Informatics-Computing Technology, Intelligent Technology, Industrial Information Integration (ICIICII). 2016. IEEE.
16. Rawlinson, K., Hp study reveals 70 percent of internet of things devices vulnerable to attack. HP, July, 2014. **29**.

17. Bertino, E. Data privacy for IoT systems: concepts, approaches, and research directions. in 2016 IEEE International Conference on Big Data (Big Data). 2016. IEEE.
18. Barth, S. and M.D. De Jong, The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. Telematics and Informatics, 2017. **34**(7): p. 1038-1058.
19. Acquisti, A. and J. Grossklags, *Privacy and rationality in individual decision making*. IEEE security & privacy, 2005. **3**(1): p. 26-33.
20. Spiekermann, S., J. Grossklags, and B. Berendt. E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. in Proceedings of the 3rd ACM conference on Electronic Commerce. 2001. ACM.
21. Morando, F., R. Iemma, and E. Raiteri, Privacy evaluation: what empirical research on users' valuation of personal data tells us. Internet Policy Review, 2014. **3**(2).
22. Norberg, P.A., D.R. Horne, and D.A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors.* Journal of Consumer Affairs, 2007. **41**(1): p. 100-126.
23. Cohen, D. and B. Crabtree, Qualitative research guidelines project. 2006.
24. Bilandzic, M. and J. Venable, Towards participatory action design research: adapting action research and design science research methods for urban informatics. Journal of Community Informatics, 2011. **7**(3).
25. McTaggart, R., *Principles for Participatory Action Research.* Adult Education Quarterly, 1991. **41**(3): p. 168-187.
26. Sanders, E.B.-N. and P.J. Stappers, *Co-creation and the new landscapes of design.* Co-design, 2008. **4**(1): p. 5-18.
27. Schön, D.A., *The reflective practitioner.* New York, 1983. **1083**.