Inclusive Security by Design

Pascal Knierim
Sarah Prange
Florian Alt
University of the Bundeswehr
Munich, Germany

Sebastian Feger
LMU Munich
Munich, Germany

Stefan Schneegass
University of Duisburg-Essen
Duisburg-Essen, Germany

M. Angela Sasse
Ruhr University Bochum
Bochum, Germany

Dominik Bayerl
Hans-Joachim Hof
Technical University of Ingolstadt
Ingolstadt, Germany

ABSTRACT

With the digital transformation touching all aspects of people's lives, digital security practices and shortcomings increasingly affect the physical world, with substantial consequences for human quality of life. The way digital security is currently designed is a significant barrier for many users. It creates negative user experiences and makes many people dependent on others to participate in the digital world safely. Understanding, controlling, and acting on digital security aspects is key to a self-determined life. Collaborative research is required to address this important challenge that could bring the digital transformation to a halt. This workshop aims to bring together researchers from the human-computer-interaction and security communities to build an understanding of technical and social requirements for inclusive security.

KEYWORDS

usable security, inclusion, self-determined security

1 INTRODUCTION

Ubiquitous computing devices proliferate in all aspects of users' everyday lives, including their homes, cars, and workplaces, but also places such as cafés, shops, or train stations. While providing great benefits and features, these devices are vulnerable to unprecedented attacks and threats, putting individuals' security at risk.

In particular, attacks cannot only target digital, but also physical assets (cf. the notion of "cyber-physical" attacks, e.g. [1, 5]). In a smart home, for example, attackers may obtain sensitive, personal user data as well as physical valuables such as costly hardware or household appliances. Even worse, they could steal treasured, irreplaceable items such as art, jewelry, or pets – which can additionally cause emotional damage regardless of their financial value.

At the same time, novel ubiquitous devices are designed with a focus on increasing users' perceived comfort through added features, resulting in little to no security mechanisms [2] or mechanisms with limited usability and user experience [3, 4].

While physical security mechanisms are often easy to use for many target groups (e.g., physical locks for cars or homes), digital security methods frequently mismatch with the primary purpose of the devices, used metaphors, and users' mental models. As a result, many individuals are overwhelmed by managing their digital security. As such, they either employ workarounds (e.g., noting down or reusing passwords, deactivating security features) or outsource security management to trusted third parties (e.g., family members).

In this workshop, we bring together researchers from the human-computer-interaction and security communities to specifically discuss *societal* aspects of security in depth. Questions of interest include: *how can security be integrated in a cyber-physical world?* and *how can security be designed to inclusively match individuals' mental models and needs?* Furthermore, we want to provide a platform to exchange opinions on *why* inclusive security is important and still a nontrivial task.

2 GOALS AND EXPECTED OUTCOME

The goal of this workshop is to bring together researchers from the human-computer-interaction and security communities. The following key aspects are of interest to the workshop:

Understanding Target Groups. IT security is becoming increasingly complex, with devices becoming more sophisticated and allow to record, store and access security relevant information. As a result, large parts of the society are excluded from digital advances, are only able to navigate insecurely in the cyber-physical world, or need to rely on external parties to support them. A key question in this workshop is: *How to design security mechanisms that are inclusive across the diverse spectrum of target groups and applications?*

Understanding Requirements. Ubiquitous computing proliferates in users' everyday lives. It is crucial to not only understand why inclusive security is important but also the *technical requirements* to overcome current limitations hindering widespread security.

2.1 Before the Workshop

A dedicated web page containing additional information about the workshop for potential attendees will be created and advertised prior to the conference. The call for papers will be distributed to the community by the organizers. In addition, we will seek reviewers to

Veröffentlicht durch die Gesellschaft für Informatik e.V.
in K. Marky, U. Grünefeld & T. Kosch (Hrsg.):
Mensch und Computer 2022 – Workshopband, 04.-07. September 2022, Darmstadt

https://doi.org/10.18420/muc2022-mci-ws14-128

serve on the program committee. To ensure high quality of accepted papers, each contribution will be examined by two reviewers in a double-blind review procedure.

2.2 During the Workshop

The workshop is a full-day event with six working hours, including a morning, lunch, and afternoon break. The preliminary workshop agenda includes a keynote, presentations from participants, interactive discussions, and a round table. The workshop will conclude with a brief summary of the overall findings and next steps.

Keynote. An invited keynote will kick off the workshop program before the presentations and interactive discussions begin. The organizing committee will invite a renowned researcher in the field of usable security and privacy to provide a forward-thinking perspective.

Presentations. Participants will be invited to write a two-page position statement and be given the opportunity to present their work in a 5-minute presentation. Participants can also submit a 250-word opinion statement and express it in our 90-second Opinion-Madness, which covers participants' ideas, visions, experiences, or opportunities and challenges addressing inclusive security.

Discussions. The workshop will be largely focused on interactive discussions centered on the topics and themes represented by the submitted position statements. These group discussions will take place following each presentation. The discussions will be moderated and facilitated by the organizers.

Round Table. During the round table session, all participants will discuss and debate in a smaller group, building on the prior conversation. We expect that participants will be able to use this format to facilitate future collaborations on inclusive security.

2.3 After the Workshop

We hope to connect scholars interested in inclusive security by design through the workshop. In addition, we intend to write an article regarding security by design. Participants who are interested in co-authoring this expected publication will be contacted. Accepted position papers will be made available on the workshop website. Drawn from the findings of this workshop, the organizers plan to apply for a DFG priority program[1] in this domain.

3 ORGANIZERS

We present the workshop organizers in the following:

Pascal Knierim is a postdoctoral researcher at the Usable Security and Privacy Group at the Research Institute CODE, University of the Bundeswehr, Munich. He obtained his PhD in Computer Science in 2020 from the Ludwig Maximilian University of Munich, where he investigated how to enhance input and output modalities for mixed reality experiences. Currently, he investigates human behavior and physiology in security-critical situations, e.g., social engineering. To protect users in the digital space, he envisions, develops and evaluates novel intervention mechanisms.

[1] https://www.dfg.de/foerderung/programme/koordinierte_programme/schwerpunktprogramme/index.html

Sebastian Feger is a postdoctoral researcher at the Human-Centered Ubiquitous Media group at LMU Munich. One of his key research threads relates to the user-centered design of systems that communicate security and privacy assessments of smart connected devices along with intervention strategies. Sebastian's research has already been applied in practice at CERN in a collaborative effort to evaluate interaction techniques in a diverse and large-scale environment.

Sarah Prange is part of the Usable Security and Privacy Group at the Research Institute CODE, University of the Bundeswehr, Munich. She is currently working on her PhD thesis on usable privacy and security in smart homes. In this context, she specifically investigated how users' awareness of privacy and security issues can be increased, as well as mechanisms to empower control over personal privacy and security.

Dominik Bayerl is a researcher at the Security in Mobility group of the Technical University of Ingolstadt, where he is working on novel methods for testing and improving the security in embedded systems. His current work focuses on applying machine learning algorithms on binary firmware code to automatically detect different types of security flaws.

Stefan Schneegaß is an assistant professor of computer science at the University of Duisburg-Essen. In 2016, he received his PhD from the University of Stuttgart. His research focuses on human-computer interaction where he works in particular on topics related to usable security such as the development of novel ways to authenticate users as well as the scalability of current approaches.

Angela Sasse holds the Chair for Human-Centred Security at the Horst Görtz Institute for IT Security at the Ruhr University in Bochum. Sasse is considered as one of the pioneers of usable security. Her research interests include human–computer interaction and computer security. She studies human-centered frameworks that explain the role of security, privacy, identity, and trust in human-technology interactions.

Hans-Joachim Hof is an experienced lead researcher with a demonstrated history of working in the security industry. He is a full professor at and vice president of the Technical University of Ingolstadt where he leads the research group "Security in Mobility" in the CARISSMA Institute for Electric, Connected, and Secure Mobility. His research group currently focuses on artificial intelligence for secure automotive software and security controls for vehicles. From 2011 till 2016, Hans-Joachim used to be a full professor at the Munich University of Applied Sciences. He led the MuSe - Munich IT Security Research Group. Well-recognized work of his group includes Secure Scrum and a design guide for usable security. Before his return to academia, Hans-Joachim was a Research Scientist in the research center Corporate Technology of the Siemens AG in Munich, Germany. His focus was on security for the Internet of Things as well as protection for smart grids and industrial networks. Well-recognized work from his time at Siemens include early work on secure wake-up receivers for wireless nodes. Hans-Joachim received a PhD from the Computer Science Department of the University of Karlsruhe, Germany. During his time at the university, Hans-Joachim researched IT security in ad-hoc and sensor networks. Well-recognized work from this time includes his work on cluster-based security architectures as well as secure bootstrapping of peer-to-peer networks.

Florian Alt is a Full Professor of Usable Security and Privacy at the University of the Bundeswehr, Munich. Florian's research is situated at the crossroads of HCI and IT security. In particular, he is interested in how knowledge on human behavior and physiology can serve to build better security-related user interfaces. Application areas of his research include behavioral biometrics, social engineering, as well as usable security and privacy mechanisms for smart homes and mixed reality.

REFERENCES

[1] Bako Ali and Ali Ismail Awad. 2018. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors* 18, 3 (2018). https://doi.org/10.3390/s18030817

[2] Florian Alt and Emanuel von Zezschwitz. 2019. Special Issue: Emerging Trends in Usable Security and Privacy. *Journal of Interactive Media (icom)* 18, 3 (dec 2019), 1–13. https://doi.org/10.1515/icom-2019-0019

[3] George Chalhoub, Ivan Flechais, Norbert Nthala, and Ruba Abu-Salma. 2020. Innovation Inaction or In Action? The Role of User Experience in the Security and Privacy Design of Smart Home Cameras. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Berkeley, CA, USA, 185–204. https://www.usenix.org/conference/soups2020/presentation/chalhoub

[4] George Chalhoub, Ivan Flechais, Norbert Nthala, Ruba Abu-Salma, and Elie Tom. 2020. Factoring User Experience into the Security and Privacy Design of Smart Home Devices: A Case Study. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '20)*. Association for Computing Machinery, New York, NY, USA, 1–9. https://doi.org/10.1145/3334480.3382850

[5] Ryan Heartfield, George Loukas, Sanja Budimir, Anatolij Bezemskij, Johnny R.J. Fontaine, Avgoustinos Filippoupolitis, and Etienne Roesch. 2018. A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security* 78 (2018), 398–428. https://doi.org/10.1016/j.cose.2018.07.011