Take Your Security and Privacy Into Your Own Hands! Why Security and Privacy Assistants Should be Tangible

Sarah Delgado Rodriguez
sarah.delgado@unibw.de
Bundeswehr University Munich, LMU Munich
Germany

Sarah Prange
sarah.prange@unibw.de
Bundeswehr University Munich, LMU Munich
Germany

Florian Alt
florian.alt@unibw.de
Bundeswehr University Munich
Germany

ABSTRACT

In the era of ubiquitous computing, users security and privacy is at risk at almost all times. Security and privacy assistants support their users in becoming aware of these risks and taking the appropriate measures to protect their data. However, they often suffer from being too complex, not intuitive and non-engaging. Hence, in order to truly enable less tech-savvy or inexperienced persons to use security and privacy assistants, we argue that such mechanisms must become *tangible* in the future.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; • **Human-centered computing** → *Ubiquitous and mobile devices.*

KEYWORDS

usable security, privacy, tangible, privacy assistant

1 INTRODUCTION & BACKGROUND

Connected devices are increasingly ubiquitous in our lives, as they are integrated into both, our surroundings and everyday routines. However, besides all the benefits these devices entail, they also put our privacy at risk. Users of such technologies often disclose much more information about themselves than they realize or are unable to properly assess potential risks to their sensitive data [6–8, 17, 19, 20]. The protection of one's own data and privacy should, therefore, be of interest to everyone. However, concepts related to security and privacy are often complex and intangible for users. Hence, researchers frequently suggest assisting users through transparent awareness mechanisms and easy to use control functionalities [4, 9, 23]. Nevertheless, the resulting privacy and security assistants frequently target individuals who can interpret and apply the corresponding variety of information and configurations [18]. This can lead to large usability and trust barriers, for example for bystanders (e.g. visitors), less tech-savy or less experienced users [1, 7–9]. Moreover, researchers observed mistrust in software controls and a desire for physical, unambiguous and easy to use alternatives [1, 2, 24]. We, therefore, argue that in the future, such mechanisms need to be tangible in order to make them truly engaging, trust inspiring and intuitive. Tangible interactions enable *direct, integrated* and *meaningful* control and communication of data [21], making them the ideal basis for both, awareness and control functionalities of security and privacy assistants. Such envisioned tangible assistants materialize the abstract concepts of security and privacy, making them physically graspable and directly manipulable, and thereby support the formation of mental models and reduce cognitive load. To support our claim, we have compiled a selection of possible research areas and open questions on tangible security and privacy assistants.

2 RESEARCH AREAS

In the following, we list three exemplary future research areas for tangible security and privacy assistants. Please note that the actual field of possible research is much larger.

2.1 Authentication

Authentication mechanisms generally include secret-, token- and biometric-based approaches. Tangible interactions could be applied to any of these mechanisms, but also to combined approaches. To generate tangible input and output, an additional object or dedicated hardware is usually required. Hence, related work suggested using these interactive objects as authentication tokens [3, 22]. Researchers further investigated tangible, interactive objects and gestures performed with them as secret-based [10, 11, 13] or behavioral biometric [16] authentication methods. We, therefore, envision a tangible security assistant that uses explicit input (e.g. rotation or button press) and behavioral measurements (e.g. acceleration, touch sensing) for secure and engaging multi-level authentication on connected objects.

2.2 Privacy in the Internet of Things

Tangible assistants that allow to configure and enforce personal privacy choices in smart environments have been suggested multiple times in recent works, but have been scarcely implemented to the date [1, 14, 15]. Such systems increase awareness by informing users on nearby sensor enhanced IoT devices (e.g. cameras or microphones). Furthermore, they enable users to accept or reject the data collection to a certain degree. Nevertheless, researchers found that intangible solutions suffer from mistrust and excessive complexity, especially for bystanders (e.g. visitors or non-users) and less experienced or non-techy individuals [1, 17]. Hence, we argue that the development of tangible privacy assistants is urgently needed, as more and more sensors are being installed in both, novel (e.g. smart home devices or drones) and traditional (e.g. PC) devices.

Mensch und Computer 2021, Workshopband , 14. Workshop Be-greifbare Interaktion

https://doi.org/10.18420/muc2021-mci-ws09-393

2.3 Online Security

Moreover, tangible interactions could assist users online by increasing their awareness of security critical situations. Researchers found that warnings are commonly ignored due to habituation [12]. However, tangible feedback like vibration or movement might be harder to ignore and easier to distinguish from the large variety of other notifications. For instance, such stimuli can be generated by an uncommon or external device, like a wrist band, enhanced glasses or a physical keyboard (similar to the "moody" keyboard [5]).

3 CONCLUSION

We argue that security and privacy assistants should be tangible, to be really usable by everybody (i.e. especially bystanders, non-tech-savy or less experienced users). We, therefore, discussed three exemplary research areas – authentication, privacy in the internet of things and online security – where we see a special potential for tangible interactions. Interesting questions for future research include, but are not limited to, how to 1) design tangible input and output mechanisms for *authentication*; 2) design tangible *privacy mechanisms* that support the needs of various target groups; and 3) design tangibles to foster *awareness* for security and privacy critical situations. We are looking forward to discuss these, further application areas and potential limitations in the workshop panel.

ACKNOWLEDGMENTS

The presented work was funded by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr [MuQuaNet].

REFERENCES

[1] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2020. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW2, Article 116 (Oct. 2020), 28 pages. https://doi.org/10.1145/3415187

[2] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. "It Did Not Give Me an Option to Decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 555, 16 pages. https://doi.org/10.1145/3411764.3445691

[3] YuQun Chen and Michael Sinclair. 2008. Tangible Security for Mobile Devices. In *Proceedings of the 5th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services* (Dublin, Ireland) *(Mobiquitous '08)*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Brussels, BEL, Article 19, 4 pages. https://doi.org/10.4108/ICST.MOBIQUITOUS2008.3936

[4] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. 2020. Informing the Design of a Personalized Privacy Assistant for the Internet of Things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376389

[5] Alexander De Luca, Bernhard Frauendienst, Max Maurer, and Doris Hausen. 2010. On the Design of a "Moody" Keyboard. In *Proceedings of the 8th ACM Conference on Designing Interactive Systems* (Aarhus, Denmark) *(DIS '10)*. Association for Computing Machinery, New York, NY, USA, 236–239. https://doi.org/10.1145/1858171.1858213

[6] Rachna Dhamija, J. D. Tygar, and Marti Hearst. 2006. Why Phishing Works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Montréal, Québec, Canada) *(CHI '06)*. Association for Computing Machinery, New York, NY, USA, 581–590. https://doi.org/10.1145/1124772.1124861

[7] Batya Friedman, David Hurley, Daniel C. Howe, Edward Felten, and Helen Nissenbaum. 2002. Users' Conceptions of Web Security: A Comparative Study. In *CHI '02 Extended Abstracts on Human Factors in Computing Systems* (Minneapolis, Minnesota, USA) *(CHI EA '02)*. Association for Computing Machinery, New York, NY, USA, 746–747. https://doi.org/10.1145/506443.506577

[8] Radhika Garg and Christopher Moreno. 2019. Understanding Motivators, Constraints, and Practices of Sharing Internet of Things. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 3, 2, Article 44 (June 2019), 21 pages. https://doi.org/10.1145/3328915

[9] Almut Herzog and Nahid Shahmehri. 2007. User Help Techniques for Usable Security. In *Proceedings of the 2007 Symposium on Computer Human Interaction for the Management of Information Technology* (Cambridge, Massachusetts) *(CHIMIT '07)*. Association for Computing Machinery, New York, NY, USA, 11–es. https://doi.org/10.1145/1234772.1234787

[10] Ho-Man Colman Leung, Chi-Wing Fu, and Pheng-Ann Heng. 2018. TwistIn: Tangible Authentication of Smart Devices via Motion Co-Analysis with a Smartwatch. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 2, Article 72 (July 2018), 24 pages. https://doi.org/10.1145/3214275

[11] Sana Maqsood, Sonia Chiasson, and Audrey Girouard. 2016. Bend Passwords: Using Gestures to Authenticate on Flexible Devices. *Personal Ubiquitous Comput.* 20, 4 (Aug. 2016), 573–600. https://doi.org/10.1007/s00779-016-0928-6

[12] Jo-Mae Maris and Tarek Amer. 2007. Signal Words and Signal Icons in Application Control and Information Technology Exception Messages—Hazard Matching and Habituation Effects. *Journal of Information Systems* 21 (09 2007). https://doi.org/10.2308/jis.2007.21.2.1

[13] Karola Marky, Martin Schmitz, Verena Zimmermann, Martin Herbers, Kai Kunze, and Max Mühlhäuser. 2020. 3D-Auth: Two-Factor Authentication with Personalized 3D-Printed Items. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376189

[14] Vikram Mehta, Arosha K. Bandara, Blaine A. Price, and Bashar Nuseibeh. 2016. Privacy Itch and Scratch: On Body Privacy Warnings and Controls. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 2417–2424. https://doi.org/10.1145/2851581.2892475

[15] Vikram Mehta, Arosha K. Bandara, Blaine A. Price, Bashar Nuseibeh, and Daniel Gooch. 2021. Up Close & Personal: Exploring User-Preferred Image Schemas for Intuitive Privacy Awareness and Control. In *Proceedings of the Fifteenth International Conference on Tangible, Embedded, and Embodied Interaction* (Salzburg, Austria) *(TEI '21)*. Association for Computing Machinery, New York, NY, USA, Article 7, 13 pages. https://doi.org/10.1145/3430524.3440626

[16] Martez Mott, Thomas Donahue, G. Michael Poor, and Laura Leventhal. 2012. Leveraging Motor Learning for a Tangible Password System. In *CHI '12 Extended Abstracts on Human Factors in Computing Systems* (Austin, Texas, USA) *(CHI EA '12)*. Association for Computing Machinery, New York, NY, USA, 2597–2602. https://doi.org/10.1145/2212776.2223842

[17] Sarah Prange, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. 2021. PriView– Exploring Visualisations to Support Users' Privacy Awareness. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, Article 69, 18 pages. https://doi.org/10.1145/3411764.3445067

[18] William Seymour, Martin J. Kraemer, Reuben Binns, and Max Van Kleek. 2020. Informing the Design of Privacy-Empowering Tools for the Connected Home. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376264

[19] Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I. Hong. 2020. I'm All Eyes and Ears: Exploring Effective Locators for Privacy Awareness in IoT Scenarios. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376585

[20] Sarina Till and Melissa Densmore. 2019. A Characterization of Digital Native Approaches To Mobile Privacy and Security. In *Proceedings of the South African Institute of Computer Scientists and Information Technologists 2019* (Skukuza, South Africa) *(SAICSIT '19)*. Association for Computing Machinery, New York, NY, USA, Article 22, 9 pages. https://doi.org/10.1145/3351108.3351131

[21] Elise van den Hoven, Evelien van de Garde-Perik, Serge Offermans, Koen van Boerdonk, and Kars-Michiel H. Lenssen. 2013. Moving Tangible Interaction Systems to the Next Level. *Computer* 46, 8 (2013), 70–76. https://doi.org/10.1109/MC.2012.360

[22] Rosa van Koningsbruggen, Bart Hengeveld, and Jason Alexander. 2021. *Understanding the Design Space of Embodied Passwords Based on Muscle Memory*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445773

[23] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300428

[24] 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.