Usable Authentication in Multi-Device Ecosystems

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

Karola Marky
Technical University of Darmstadt,
Germany,
University of Glasgow
Scotland
marky@tk.tu-darmstadt.de

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

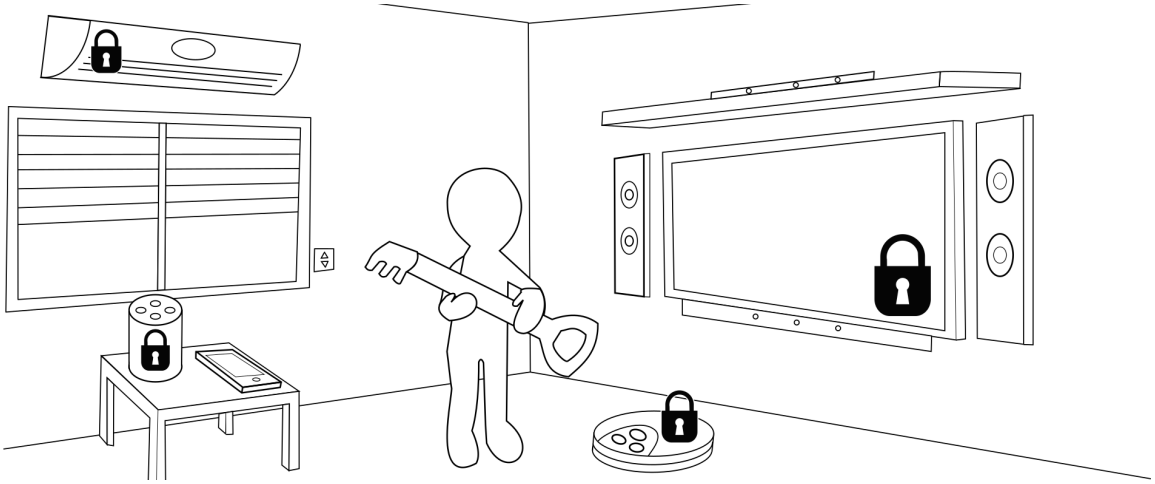

Figure 1: In this position paper, we discuss challenges for usable authentication in multi-device environments.

ABSTRACT

A plethora of "smart" devices pervades users' daily lives and, more precisely, their homes. While these devices provide a rich variety of features and benefits to users (e.g., fostering automation), they more importantly also collect, store and process sensitive user data. However, suitable security and privacy mechanisms for such devices are still scarce. In this position paper, we discuss challenges of usable authentication in multi-device ecosystems.

CCS CONCEPTS

• **Security and privacy** → **Authentication**; • **Human-centered computing** → *Ubiquitous and mobile devices*; Interaction techniques.

KEYWORDS

Smart Home, Smart Devices, IoT, Interaction, Ubiquitous Computing, Authentication

ACM Reference Format:
Sarah Prange, Karola Marky, and Florian Alt. 2021. Usable Authentication in Multi-Device Ecosystems. In *CHI 2021 Workshop on User Experience for Multi-Device Ecosystems: Challenges and Opportunities.* ACM, New York, NY, USA, 3 pages.

CHI '21, May 8–13, 2021, Yokohama, Japan

1 INTRODUCTION

An increasing number of devices pervades users' everyday life and, more precisely, their homes. Smart home devices come in various form factors [11] and provide a plethora of features and benefits to users, e.g., supporting home automation or sustainable energy consumption (cf. [9] for an overview). To provide this functionality, smart devices and associated services collect, store, and process – potentially sensitive – user data, which opens a need for protection (cf. Figure 1). Think about, e.g., a smart voice assistant that is connected to a user's online shopping profile as well as to many other services within the home. However, security mechanisms are rarely implemented on smart devices on the consumer market [8]. If implemented, such mechanisms are of limited user experience [1, 2]. Think about, e.g., entering a secure password on a remote control to log into a video streaming platform on the TV. To close this gap, we argue that authentication in multi-device ecosystems should seamlessly blend with how users naturally interact with the devices.

In this position paper, we first illustrate the need for authentication in smart home ecosystems and existing approaches. We then discuss challenges of usable authentication in multi-device scenarios and set out directions for future research.

2 MOTIVATION & BACKGROUND

In this section, we first illustrate potential attacks and threats as well as a few smart home scenarios, which make authentication indispensable. We then discuss how authentication mechanisms for multi-device ecosystems might look like.

2.1 Attacks & Threats

Smart home devices are vulnerable to novel attacks and threats [14], which becomes especially critical as we let those devices enter our homes. Examples include, but are not limited to, remote network attacks or leakage of data captured by the devices [14]. Consequences of attacks towards home setups are severe as attackers might not only virtually, but also physically access our homes. Related work highlighted two major types of adversaries that are specific to smart homes, namely *remote* and *inside* attackers [5]. Inside attackers have legitimate physical access to the home (e.g., household members or temporary workers).

2.2 Authentication in Smart Homes

Within the home, many scenarios (should) require users to authenticate in one or the other way. Some of these scenarios involve *one* or *multiple* devices within the home:

Coming Home. When coming home, users usually unlock the door using a *physical key*. Subsequently, users have (physical) access to *all devices* in their home system. A conventional, physical attacker might get hold of a key or break the door lock to gain this access.

Device Configuration. When using a *single device*, users might need to authenticate towards this device to prevent illegitimate users from manipulating settings.

Moreover, many smart devices in users' homes provide access to *external services* that exist beyond the multi-device ecosystem and require authentication.

Watching Series. When accessing their favorite streaming service via a smart TV, users need to provide credentials. This often requires users to enter a conventional *password* on the TV's remote control, which clearly is a frustrating experience. As a result, this procedure is oftentimes required on first use only, which is not optimal from a security perspective.

Alexa goes shopping. Voice assistants, such as Amazon's Alexa, allow placing orders. While purchases can be protected via a *voice PIN*, this might be overheard and exploited by, e.g., family members [6] or guests.

2.3 Authentication Mechanisms for Smart Devices

Albeit being necessary (cf. previous section), security mechanisms on current consumer devices are scarce [8] and/or of limited user experience [1, 2]. Oftentimes, desktop metaphors are being transferred [5] to smart devices – resulting in, e.g., entering passwords on a TV's remote control. While knowledge-based authentication mechanisms are suitable for a one-user-one-device relationship, they do not scale to multi-device ecosystems due to a) the immense number of devices, accounts and passwords exceeding users' memorability and b) many devices missing suitable input modalities for conventional mechanisms, such as passwords. Furthermore, knowledge-based mechanisms are prone to shoulder surfing [4] or guessing attacks. Biometric mechanisms based on, e.g., users' face or voice, or behavior, offer opportunities for a more seamless approach, but are often used for personalization (e.g., customizing reminders) rather than for security purposes [5]. Moreover, voice commands for authentication might be overheard by an attacker [6].

Prior research discussed whether authentication mechanisms in multi-device environments should focus on one device, or rather on the whole ecosystem [11]. While in some cases authenticating towards only one device within the ecosystem might make sense (e.g., authenticating at a smart fridge prior to a purchase), many single devices do not provide suitable modalities and many use cases within the home involve multiple devices at once. As an example, for watching a movie, users might access their preferred video streaming platform via their smart TV, but also have a particularly preferred light, temperature and sound setup that should not be accessed or manipulated by third parties.

Sample authentication mechanisms have been suggested, e.g. identifying users by their operations with multiple devices [7]. While this currently requires workarounds, such as users wearing a wristband to employ virtual sensing [7] or additional capacitive sensing on existing devices [3], a future vision of this could be seamlessly integrated. As an example, an increasing amount of devices is equipped with technology to recognize users' interaction with them (e.g., by means of touch or motion sensors). This could be leveraged for explicit or implicit authentication. The former approach would require users to explicitly enter a "secret" by interacting with multiple devices. The latter would identify users by the way in which they interact with multiple devices.

3 CHALLENGES & DIRECTIONS FOR FUTURE RESEARCH

3.1 Seamless Authentication in Multi-Device Ecosystems

Authentication in multi-device ecosystems is challenging due to several reasons. First and foremost, conventional mechanisms are imposed to novel devices, leading to a mismatch between the devices' affordances and the mechanisms' input requirements. Secondly, conventional authentication mechanisms do not scale to multi-device environments, as, e.g., remembering a secret for each and every device or service would clearly exceed users' memory capabilities. While research suggests an increasing number of novel mechanisms for ubiquitous devices [12], the existence of multiple devices as well as multiple users is still poses a challenge. Lastly, multi-device ecosystems are often multi-task environments. Originally, authentication in ubiquitous computing is a secondary task (e.g., unlocking the phone before continuing with the main task, calling a friend). However, interacting with multiple devices allows for multiple tasks (e.g., controlling music, heating and lights at once), in which authentication needs to fit in. This raises the question: *How can authentication in a multi-device ecosystem blend with users' natural interaction to be usable as well as secure?*

3.2 Privacy in Multi-Device Ecosystems

While security clearly is a challenge, preserving users' privacy in multi-device ecosystems is also not trivial. Firstly, interactions, such as gestures, might be overseen or voice commands overheard. Secondly, multi-device ecosystems oftentimes involve multiple users as well. Examples are co-inhabitants, family members, or guests.

To prevent personal data being accessed by others, mechanisms to set fine-grained permissions are necessary. Thirdly, users are oftentimes unaware of their data being collected by multiple devices. Mechanisms to increase awareness have been suggested [10, 13]. Lastly, combining the data captured by multiple devices within the ecosystem leads to entirely new information about users. For instance, a lightning system in itself captures on/off states, but can, together with, e.g., thermostat data and fridge content, reveal if and how many users are currently present. This raises the question: *How can multi-device ecosystems be designed in such a way that they protect users' privacy, while preserving the primary user experience?*

4 CONCLUSION

With this position paper, we address the workshop call for challenges for multi-device user experience, with particular focus on authentication. We hope to stimulate a discussion at the workshop as to how usable authentication in multi-device ecosystems can be designed, and how users' privacy can be protected in such scenarios.

REFERENCES

[1] 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, 185–204. https://www.usenix.org/conference/soups2020/presentation/chalhoub

[2] 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

[3] Sarah Delgado Rodriguez, Lukas Prange, Sarah an Mecke, and Florian Alt. 2021. ActPad – A Smart Desk Platform to Enable User Interaction with IoT Devices. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI EA '21)*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411763.3451825 to appear.

[4] Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 4254–4265. https://doi.org/10.1145/3025453.3025636

[5] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. 2018. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, Baltimore, MD, 255–272. https://www.usenix.org/conference/usenixsecurity18/presentation/he

[6] William Jang, Adil Chhabra, and Aarathi Prasad. 2017. Enabling Multi-User Controls in Smart Home Devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy* (Dallas, Texas, USA) *(IoTS&P '17)*. Association for Computing Machinery, New York, NY, USA, 49–54. https://doi.org/10.1145/3139937.3139941

[7] Xiaopeng Li, Fengyao Yan, Fei Zuo, Qiang Zeng, and Lannan Luo. 2019. *Touch Well Before Use: Intuitive and Secure Authentication for IoT Devices.* Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3300061.3345434

[8] Shrirang Mare, Logan Girvin, Franziska Roesner, and Tadayoshi Kohno. 2019. Consumer Smart Homes: Where We Are and Where We Need to Go. In *Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications* (Santa Cruz, CA, USA) *(HotMobile '19)*. Association for Computing Machinery, New York, NY, USA, 117–122. https://doi.org/10.1145/3301293.3302371

[9] Davit Marikyan, Savvas Papagiannidis, and Eleftherios Alamanos. 2019. A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change* 138 (2019), 139 – 154. https://doi.org/10.1016/j.techfore.2018.08.015

[10] Sarah Prange, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. 2021. PriView – Exploring Visualisations Supporting Users' Privacy Awareness. 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. https://doi.org/10.1145/3313831.3376840 to appear.

[11] Sarah Prange, Emanuel von Zezschwitz, and Florian Alt. 2019. Vision: Exploring Challenges and Opportunities for Usable Authentication in the Smart Home. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 154–158. https://doi.org/10.1109/EuroSPW.2019.00024

[12] S. W. Shah and S. S. Kanhere. 2019. Recent Trends in User Authentication – A Survey. *IEEE Access* 7 (2019), 112505–112519. https://doi.org/10.1109/ACCESS.2019.2932400

[13] 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

[14] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu. 2019. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet of Things Journal* 6, 2 (2019), 1606–1616. https://doi.org/10.1109/JIOT.2018.2847733