Vision: Exploring Challenges and Opportunities for Usable Authentication in the Smart Home

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

Emanuel von Zezschwitz
University of Bonn
Bonn, Germany
zezschwitz@cs.uni-bonn.de

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

***Abstract*—In this work, we explore designs and possible threats of current smart home environments to support the design of novel authentication mechanisms. Our work is motivated by the ever increasing number of smart devices in people's homes that are meant to enhance users' daily life. Examples for such devices include, but are not limited to, smart TVs, cleaning robots, devices for health and well-being, as well as for cooking. Such devices are capable of collecting sensitive data and subsequently derive information, for example, whether a user is at home, how often they cook or watch TV, etc. To understand possible threats emerging from smart devices being capable of accessing sensitive data, we first chart a design and problem space. Our work is complemented by an in-depth discussion on future research directions and challenges as well as how threats can be mitigated by visionary novel authentication approaches.**

***Index Terms*—smart home, smart devices, authentication, usable security, threat models, privacy**

I. Introduction

Smart home devices are entering the market at a rapidly accelerating pace. Such devices collect and allow access to sensitive data. At the same time, suitable authentication mechanisms are still scarce. Yet they will become increasingly important as more devices proliferate in our homes.

Current designs of smart home devices either ignore authentication, require a one-time authentication only (e.g., setting up the Netflix account for the smart TV) or provide workarounds in the form of smartphone apps, which oftentimes serve as the only interface to the device(s). However we rarely see authentication mechanisms specifically designed for smart devices with particular (uncommon) form factors or user interfaces. We see a large opportunity here: smart devices add novel means for input (e.g., touch interfaces, speech, etc.), come with novel output devices (haptic feedback, audio, etc.), and are networked. These properties can be leveraged by designers of smart home devices, to build novel authentication concepts – in particular such that adhere to Nielsen's postulate for security mechanisms designed for the way in which people behave[1].

In this work, we contribute to realising this vision in several ways. Firstly, we chart a design space for smart home devices. This design space is meant to summarise aspects that are important in the context of authentication. Secondly, we present a problem space that briefly summarises potential threats to smart home authentication mechanisms. We then suggest an approach that allows designers to assess possible threats to which their devices are potentially exposed. Ultimately, we present two high-level authentication concepts that we envision for smart homes: (a) device-centric authentication mechanisms, and (b) home-centric authentication. We conclude with a discussion of challenges related to these two concepts.

With our work, we hope to stimulate a discussion regarding the design of smart home authentication mechanisms. We see a large opportunity to design novel mechanisms that blend with the way how users interact in smart homes, hence making them not only secure, but also highly usable.

[1]https://www.nngroup.com/articles/security-and-human-factors/, last accessed 03-12-2019

II. Background

To set the scene for our work, we will provide a brief introduction to smart environments, authentication and threats.

A. Smart Homes & Devices

We define a smart home as providing an "intelligent living environment for daily convenient life" [1]. Moreover, a smart home is a home characterised by a number of Internet of Things (IoT) devices and household appliances that can be controlled automatically and remotely [2], [3]. Such a setup typically comprises the following components: a smart central controller, several switch modules to access various devices (e.g., lighting, fridge) or values (e.g., temperature), and a connection to the internet for remote access and control [4]. In particular, smart devices are "[...] capable of communication and computation, ranging from simple sensor nodes to home appliances and sophisticated smart phones" [5].

B. Interaction in Smart Homes

Interaction with a smart home and its devices is challenging due to a) an arbitrary number of devices to control and b) multiple users of several target groups. Interaction with multiple devices or by multiple users may happen concurrently.

To address this, Beigl suggests an appliance to point at the desired device first and control it afterwards [6]. User-defined gesture approaches have been additional subject to research [7]. Novel approaches include trigger-action programming for smart home control [8]. Further interaction modalities include, but are not limited to, touch, voice or tangibles.

Due to limited UIs (e.g., lack of keyboard or display) on the smart devices themselves, they are often controlled via a central unit (e.g., the smartphone). Even though a centralised control unit for the smart home has been found beneficial in prior research [9], we hypothesise that decentralised, and thus direct interaction paradigms will be required in the future, when the number of smart devices will significantly increase.

C. Authentication Mechanisms

Typically, we distinguish three types of authentication mechanisms based on the authentication factor [10]: *Knowledge-based* authentication mechanisms require users to remember a secret; *token-based* authentication mechanisms require the use of an object, such as keys or a smart card; and *biometric* approaches identify the user based on their physiology (e.g., fingerprints) or their behaviour (gait, typing).

These authentication mechanisms are employed in various areas (e.g., smartphones, websites). Of particular interest in smart homes are online accounts, since they can be accessed via an increasing number of devices (e.g., smart TV) and make use of traditional knowledge-based factors (e.g., passwords). Other devices, such as smart speakers, may employ alternative approaches like voice biometrics[2]. However, transferring these to the smart home is challenging. Such challenges include entering secure (i.e. lengthy) passwords on remote controls (e.g., for logging into a SmartTV account), being tedious, time consuming, and annoying for users. This oftentimes leads to a single login action upon setup. Other problems may evolve from the fact that different users may have different access rights, while not being reflected by the authentication model.

D. User-Centred Threat Models

We consider user-centred threat models towards authentication, some of which may transfer to smart home contexts:

- *Guessing attacks:* an impostor tries to guess a secret [11].
- *Observation attacks:* Attacker try to observe users while entering their secrets. One of the most common observation attacks is shoulder surfing [12].
- *Social engineering:* Such attacks are characterised by trying to get credentials from users directly, e.g., by means of a phishing email. Some types of authentication mechanisms (e.g., knowledge-based approaches) are more prone to such attacks than others (e.g., biometrics).
- *Reconstruction attacks:* Attackers analyse residuals [13] or heat traces [14] to reconstruct the password.
- *Mimicry:* Attackers try to fool an authentication mechanism by pretending to be a legitimate user, for example by mimicking their behaviour [15].

As a consequence, attacks on smart homes may not only comprise gaining knowledge about the authentication and breaking the authentication mechanism, but also result in "analogoues" (i.e. physical) attacks on the victim's home (e.g., burglary). This offers an even more special need for protection, and hence secure and usable authentication mechanisms.

[2]https://support.google.com/googlehome/answer/7342711?hl=en, last accessed 03-13-2019

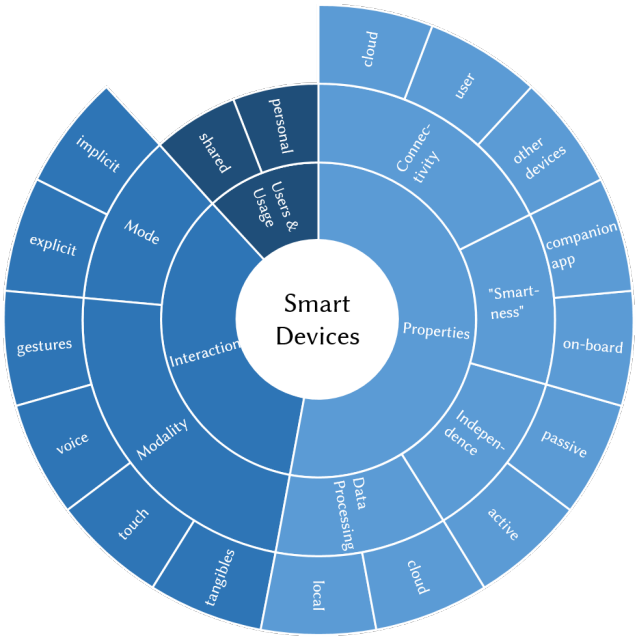

Fig. 1. Design Space: Dimensions of current smart devices that may a) possibly serve as vulnerable point for an attack and/or b) may be employed for existing as well as novel authentication mechanisms.

For many of the aforementioned threats, a prerequisite is access to the device of the user. We believe that such "local attackers" occur frequently in smart homes, e.g., among family members as well as during parties or while people rent out their homes via AirBnB.

III. Design Space: Current Smart Home Devices

To better understand characteristics and properties of smart home devices and their implications on security, we chart a design space in the following (cf. Fig. 1). We are particularly interested in characteristics that a) would allow for a suitable authentication and/or b) expose the device to potential attacks.

A. Users & Usage

Unlike many ubiquitous computing devices, smart home devices may not be used exclusively (i.e., *personal* by a single users), but be naturally *shared* between small groups (e.g., families, flatmates, etc.). This poses additional challenges, such as the need to enable switching accounts, increasing number of logins, etc.

B. Interaction

1) Mode: The mode of interaction for traditional home appliances is traditionally *explicit* (e.g., a person turning on the light when coming home). With devices becoming "smart", *implicit* interaction may become more frequent (e.g., the light turns on automatically as users enter a room).

2) Modalities: As highlighted in section II-B, several interaction modalities exist in the smart home, including, but not limited to, *gestures*, *voice*, *touch*, and *tangibles*. This offers potential for input of knowledge-based authentication, but also (physiological as well as behavioural) biometrics.

C. "Smart" Properties

While an increasing number of consumer devices is called "smart", only few of them offer "intelligent" features. In the context of this work, we consider a home device to be smart if it has the following properties:

1) Connectivity: Many components of a smart home provide some form of connectivity. They may be connected with the *cloud* (i.e. the provider), the *user* (e.g., for remote control or feedback), or *other devices* in the same environment. This allows for, e.g., sending and receiving data or commands.

2) "Smartness": The actual "smartness" (i.e. what distinguishes the "smart" device different from its "stupid" companions) may be built-in the device (*on-board)* or accessible via a *companion application* (e.g., on the smartphone).

3) Independence: Smart devices act on several levels of independence: while some devices are *passive* components (e.g., sensors collecting data about air quality), others are *active*, allowing for input and control (e.g., light controls), or even act independently (e.g., smart thermostat controls heating to save energy while keeping the desired temperature).

4) Data Processing: Smart devices may collect and/or process data. This may happen *locally* to, e.g., regulate heating or *cloud*-based to, e.g., process speech input. Sending or receiving data may serve several purposes, including, but not limited to, automation of the home or analysis by the provider.

Summary. This list of design characteristics is not exhaustive. We choose characteristics that we believe are vulnerable to (existing or novel) threat models. We discuss potential threats in the following section IV.

IV. Problem Space: Potential Threats on Authentication in the Smart Home

Regarding the design of current smart home devices, we now discuss if and how threats may transfer to smart home settings and offer a need for suitable authentication mechanisms.

Guessing Attacks. Lots of smart home devices come with predefined security settings (e.g., default passwords in routers). An attacker could probably guess standard passwords to break such a smart home system quite easily.

Observation Attacks. Regarding the various modalities in the smart home, observation may not only include visuals (i.e. watching touch or gesture input), but also audio (i.e. listening to voice input). Novel threat models may evolve around the given properties of smart devices by misusing their intended "smart" functionality for observation. As an example, smart speaker's microphones could not only be used to listen for keywords and commands, but also to listen to conversations or to gain knowledge about authentication.

Social Engineering. A smart home offers multiple attack points for social engineering due to being open for a certain group of attackers (e.g., family members, guests, couch surfers). Social engineering is more likely in a home scenario as people are naturally interacting with and know each other.

Reconstruction Attacks. By analysing residuals on smart devices, an attacker may gain access to the device and its data. We know such attacks from smartphones, but may see similar threats on smart home devices. Especially in a smart home scenario, where devices are in close proximity and easily in reach, input may be analysed shortly after the authentication process. As an example, keyboard input on a remote control could be analysed by smudge [13] or thermal [14] attacks.

Mimicry Attacks. If a smart home refers to implicit, biometric mechanisms, attackers could get access by applying mimicry attacks. This may especially be applicable if the smartphone and its sensors (e.g., fingerprint, face recognition, on-body detection) serve as means for authentication to access the smart home components.

Summary. This list is not exhaustive, but is meant to demonstrate that threat models, as known from public environments, are not only possible in smart homes, but even more likely. In addition, novel threats may emerge as smart devices with new properties and features enter our homes.

V. Assessing Possible Threats in the Smart Home

Our design and problem space can now serve as a basis to assess the vulnerability of existing smart devices and to support the design of novel devices and authentication mechanisms. In particular, designers could apply the following procedure to reflect on design characteristics and threats.

Positioning the smart device in the design space. In a first step, designers position their smart device in the design space. For example, a smart device may be interacted with explicitly, by means of voice, processes data locally, and so on (examples can be found in Table I).

Assessing possible threats. In a second step, designers then assess how each property (e.g., the used interaction modality) influences the risk for a successful attack. For example, a smart home device using voice would make it vulnerable to eavesdropping a password but not to a reconstruction attack.

The mentioned assessment is possible in many ways. In its simplest form, designers can for each property / threat combination provide a qualitative assessment in the form of a textual description. Another approach would be to calculate a score. For example, given a certain interaction modality (speech, voice, gestures, touch), the designer could rate its risk to be successfully attacked by means of one of the different threats on a scale from 1–10. Note, that our goal is not to contribute to risk assessment. Rather our approach enables different risk assessment approaches to be applied. Ultimately, an informed decision regarding design can be made.

When applying the aforementioned procedure, designers may want to consider the following aspects and challenges:

Personal and Shared Use. In contrast to many other ubiquitous devices (e.g., smartphones and smartwatches), smart home devices are meant to serve multi-user scenarios from design. Hence, we do not only face *personal*, but also *shared*

usage. While for non-shared devices, potential threats are comparable to other personal devices (e.g., shoulder surfing for password entry on smartphones), higher risks may evolve around shared devices. Since a switch between users may require multiple login actions, the "point of failures" increase. This not only refers to "human factors" (e.g., multiple users potentially failing to keep authentication secret), but also more possibilities for observation and social engineering attacks.

Mode and Modality. Depending on the interaction *mode* and *modality* of the smart device, different attacks may (not) be possible. E.g., observing touch input may be easily possible while observing gesture or biometric input may be difficult to impossible, especially when "hidden" in the users' home.

Connectivity, Smartness, and Independence. Moreover, we see high potential for attacks with regards to the "smart" features of home devices. *Connectivity* may allow for system-side attacks on the connection itself (e.g., man-in-the-middle or replay attacks). Depending on the root of *"smartness"*, malware may be placed a) in the companion app or b) the device may be victim to threats itself. The higher the device's *independence* and active action in the smart home, the higher the potential risk (being influenced by an attacker, devices may have active undesired influence). For passive smart home components, threats may concern the collected data, and only later lead to active impact in the victim's home.

VI. Approaches & Future Research Directions

For novel smart home devices, usable security should be integrated by design, i.e. smart devices of the future should provide feasible, built-in authentication mechanisms, which are seamless and intuitive. These may include conventional methods like PINs and passwords, but may also introduce novel, device or home centric mechanisms based on interaction behaviour, behavioural patterns and routines or chains of device usage.

A. Device-Centric Authentication

Conventional authentication usually happens on a single device (e.g., logging in to a laptop) or service (e.g., logging in to use Netflix). We envision transferring this to arbitrary (smart) devices to be beneficial since it fits users' mental model of "unlocking" a device before usage. To enhance security, additional mechanisms could likewise be transferred to smart devices. As an example, a smart speaker could ask dynamic security questions (similar as proposed by [16]) before accessing personal content.

However, using conventional mechanisms does not overcome certain threats (e.g., listening to voice input) or may even create new ones (e.g., observing input at the smart door may enable burglary). Moreover, input modalities in smart environments are varying and may limit possible authentication factors (i.e. not every device allows for entering a PIN via a numpad). In addition, struggling with having to remember passwords for various online accounts, remembering different input modalities may put additional burden on users. This could be addressed by a) using the same mechanism for several devices (which obviously again obscures security by creating another "single point of failure") or b) switching to other devices in the smart environment. As an example, the smartphone oftentimes serves as a hub and workaround for protecting the smart device. Additional devices can offer means for token-based (e.g., token rings) or biometric (e.g., fingerprint sensors) authentication. Some smart devices already offer additional input devices (e.g., remote controls for smart TVs), where input authentication could be integrated.

B. Home-Centric Authentication

A smart home usually comes with several "smart" components, which are *connected*. While this is on one hand vulnerable, it on the other hand offers opportunities for future, scalable authentication in the smart home by using a combination of these for authentication, while still preserving usability as well as security. The smart home and its devices as a whole could serve for authentication in several ways. The (*explicit*) input for authentication could be done on several instead of on a single device. As an example, a secret input could consider the smart TV's remote control, light switch, and smartphone.

Moreover, we can also imagine *implicit* authentication in the smart home. Such an authentication mechanism would for example consider "natural" interaction with several devices in a certain context (i.e., switching on a certain light and TV channel when user comes home from work).

Using the whole smart home for authentication comes with several benefits. It is scalable and easily expandable (i.e. not limited to the devices currently present in the smart home). It is highly usable and seamless by avoiding additional burden, but using the "normal" user interaction for authentication. Additionally, it uses functionality a smart device provides by design (i.e., being connected with other components in the same smart home) and is thus easy to implement. It may also increase security by using *multiple factors* for authentication. As an example, an authentication mechanism could refer to chains of interaction with different devices or transfer the current level of security from one device to another.

VII. Challenges & Limitations

A. Smart Devices

Many current consumer electronic devices are titled "smart". However, this not always implies any kind of intelligence or independent action. With this work, we focus on potential vulnerable points in the design of smart home devices, in particular *interconnected* devices for future usable privacy and security research in smart home environments. However, novel threats may evolve around various ("smart") devices with various ("smart") properties and may need to be protected by novel mechanisms in the future.

B. Smart Goals

"Smart" devices can follow different goals. As an example, some devices aim at increasing efficiency (e.g., reduce power consumption by regulation standby modes etc automatically).

TABLE I
CURRENT SMART HOME DEVICES FROM THE FOLLOWING CATEGORIES: ENTERTAINMENT (SMART TV), SMART SPEAKER (ALEXA), AND CARE (ORAL-B TOOTHBRUSH). WHILE THE TV AND TOOTHBRUSH HAVE "NON-SMART" PENDANTS, ALEXA IS A NOVEL AND "SMART" DEVICE.

"Smart" Devices	*Design Properties* Connectivity	"Smartness"	Independence	Data Processing
Entertainment (Smart) TV	to diverse web services (e.g., Netflix), other devices (remote control) and to the user (their accounts, their smartphone / app)	on-board: internet connection, apps, "red button"	passive (react to input commands)	login to accounts etc
Smart Assistant Alexa	to the cloud and other devices	on-board (listening to voice commands)	passive (react to (voice) commands) and active (control other devices)	cloud processes speech
Care (Smart) Toothbrush	to companion app (which then connects to the Internet)	sensors in toothbrush, smartness in companion application	passive (pressure sensors)	in the companion app

Others aim at delivering information (e.g., Alexa reads out the weather forecast) or entertainment to users (e.g., watching Netflix series on smart TVs). Following these goals may not necessarily need to access sensitive data that deserves protection. However, those that do access any kind of personal information should be protected.

C. Security Integration at (Smart) Home

In a smart home context, interaction with devices is oftentimes only the secondary task: Hence there is a challenge in how to integrate security (i.e. authentication mechanisms) so that they are manageable with little to no attention. Potential input required for authentication should not create any overhead at all. Novel authentication mechanisms, e.g., based on behavioural biometrics, offer great potential for unintrusive, easy, and effortless authentication integrated into the interaction itself. As an example, users could be identified by the way they interact with one or multiple of their smart home devices. With regards to shared device usage, it may be sufficient as a start to verify from time to time which user (from a rather small target group such as a family) is currently active to allow for personal content or settings (e.g., café latte).

D. Assessing & Communicating Risks

Another possibility to create a secure smart home environment is to assess and communicate potential risks to users. As an example, security indicators for behavioural biometrics have been suggested in prior research [17]. For smart home devices, adequate indicators can be investigated.

VIII. CONCLUSION

We presented a design space of smart home devices, discussed potential threats as well as challenges and opportunities for novel and usable authentication mechanisms in the smart home. We explain how this can be used in the design process and discuss alternative security approaches for smart homes.

We consider our work useful for researchers as well as practitioners in the era of home environments increasingly becoming "smart". We are looking forward to discussing further ideas at the EuroUSEC workshop 2019.

REFERENCES

[1] S. S. I. Samuel, "A review of connectivity challenges in IoT-smart home," *2016 3rd MEC International Conference on Big Data and Smart City, ICBDSC 2016*, 2016.

[2] K. Bing, L. Fu, Y. Zhuo, and L. Yanlei, "Design of an Internet of things-based smart home system," *Proc. ICICIP 2011*, no. PART 2, 2011.

[3] P. P. Gaikwad, J. P. Gabhane, and S. S. Golait, "A survey based on Smart Homes system using Internet-of-Things," *4th IEEE Sponsored International Conference on Computation of Power, Energy, Information and Communication, ICCPEIC 2015*, 2015.

[4] M. Wang, G. Zhang, C. Zhang, J. Zhang, and C. Li, "An IoT-based appliance control system for smart homes," *Proc. ICICIP 2013*, 2013.

[5] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of internet of things for smart home: Challenges and solutions," *Journal of Cleaner Production*, vol. 140, pp. 1454–1464, 2017.

[6] M. Beigl, "Point & click-interaction in smart environments," in *Symposium on handheld and ubiquitous computing*. Springer, 1999.

[7] C. Kühnel, T. Westermann, F. Hemmert, S. Kratz, A. Müller, and S. Möller, "I'm home: Defining and evaluating a gesture set for smart-home control," *Int. Jour. of Hum.-Comp. Studies*, vol. 69, no. 11, 2011.

[8] B. Ur, E. McManus, M. Pak Yong Ho, and M. L. Littman, "Practical trigger-action programming in the smart home," in *Proc. CHI '14*. ACM, 2014.

[9] T. Koskela and K. Väänänen-Vainio-Mattila, "Evolution towards smart home environments: empirical evaluation of three user interfaces," *Personal and Ubiquitous Computing*, vol. 8, no. 3-4, 2004.

[10] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, no. 12, Dec 2003.

[11] J. Bonneau, "The science of guessing: analyzing an anonymized corpus of 70 million passwords," in *IEEE Symp. on Sec. and Priv.* IEEE, 2012.

[12] M. Eiband, M. Khamis, E. Von Zezschwitz, H. Hussmann, and F. Alt, "Understanding shoulder surfing in the wild: Stories from users and observers," in *Proc. CHI '17*. ACM, 2017.

[13] S. Schneegass, F. Steimle, A. Bulling, F. Alt, and A. Schmidt, "Smudge-safe: Geometric image transformations for smudge-resistant user authentication," in *Proc. UbiComp '14*. ACM, 2014.

[14] Y. Abdelrahman, M. Khamis, S. Schneegass, and F. Alt, "Stay cool! understanding thermal attacks on mobile-based user authentication," in *Proc. CHI '17*. ACM, 2017.

[15] H. Khan, U. Hengartner, and D. Vogel, "Augmented reality-based mimicry attacks on behaviour-based smartphone authentication," in *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 2018.

[16] A. Hang, A. De Luca, and H. Hussmann, "I know what you did last week! do you?: Dynamic security questions for fallback authentication on smartphones," in *Proc. CHI '15*. ACM, 2015.

[17] L. Mecke, S. Prange, D. Buschek, and F. Alt, "A design space for security indicators for behavioural biometrics on mobile touchscreen devices," in *Extended Abstracts of CHI '18*. ACM, 2018.