Interact2Authenticate: Towards Usable Authentication in Smart Environments

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

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

Submitted to *CHI 2020 Workshop on Authentication Beyond Desktops and Smartphones*. Do not cite, do not circulate.
CHI '20, April 25–30, 2020, Honolulu, HI, USA.

Abstract

Users' homes are increasingly equipped with "smart" devices, capable of collecting and processing sensitive personal data. This creates a need for authentication on these devices. At the same time, conventional authentication mechanisms are often difficult to adapt to novel contexts, for example, due to the lack of suitable input modalities. Think about a password that needs to be input to a smart TV using a remote control. To address this, we suggest *Interact2Authenticate*, a novel authentication mechanism for smart environments. Our concept integrates authentication with users' daily interactions. The idea is that users authenticate as they touch objects at different positions and in different order. For example, a secret to authenticate in a smart kitchen could consist of touching the fridge handle, a cupboard, and the coffee machine. In this paper, we introduce the concept, report on how we built the prototype, and share early insights from a usability study. We discuss lessons learnt and directions for future research.

Author Keywords

Smart Home; Usable Security; Authentication

CCS Concepts

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

Object / Device	x of 107	%
mouse	102	95.33
keyboard	102	95.33
display	101	94.40
laptop/tablet	58	54.21
headphones	47	43.93
decoration	39	36.45
speaker	39	36.45
plant	31	28.97
lamp	30	28.04
PC	27	25.23
office supplies	27	25.23

Table 1: We analysed desk pictures ($N = 107$) from an online forum to find common objects on desks. Our study setup (cf. Fig. 1) is based on these findings. We used objects that occurred in more than 20% of the pictures. Note that we used a laptop only (i.e., not an additional desktop PC) and added a coffee cup as additional, movable object.

Motivation & Background

Our homes are becoming increasingly “smart”. Networked devices with different interaction technologies (e.g., smart TVs, smart assistants, smart toothbrushes) [7] that have access to different personal information enable products promising an ever-increasing number of features for users' homes serving various purposes (e.g., energy savings or home automation) [5]. The devices' capability of collecting, processing and storing personal data opens a need to employ protection in the form of, e.g., authentication mechanisms. However, authentication is a cumbersome and annoying task for users, especially when interacting frequently with the device as it is mostly the case for home appliances. Conventional authentication mechanisms such as, e.g., passwords, may not be feasible in this context due to limited interaction modalities (e.g., entering a password for a smart TV via the remote control where the single characters need to be selected with a cursor).

In line with the vision to build usable security mechanisms in such a way that they blend with human behaviour [2], we suggest to apply users' daily interaction habits for authentication. With *Interact2Authenticate*, we transfer the idea of “three dimensional” passwords that have been suggested for virtual environments [1, 4] to the real world, i.e. to the scope of smart environments.

Concept: Interact2Authenticate

With *Interact2Authenticate*, users would authenticate by touching daily objects in their environment as they would normally do as part of their interaction habits. As an example, users might have a certain routine when coming home, such as touching the door handle to enter, turning on a specific light and leaving their jacket at the wardrobe. This specific chain of interactions, including the objects, their order as well as the precise touch positions, could authenticate users for, e.g., their smart music system. Similarly, a secret to authenticate in a smart kitchen may comprise the fridge handle, a cupboard handle, and the coffee machine.

Usability. Potential factors influencing the usability of *Interact2Authenticate* include, but are not limited to: *position* of objects (e.g., easy in reach vs far away, distance to the dominant hand); *moving* vs static objects (potentially influencing memorability); possibility to integrate the authentication secret to *usual habits* and routines.

Security. From a security perspective,*Interact2Authenticate* could consider the following metrics: *number* of involved objects; usage of *duplicate* objects; potential *touch points* per object; *dynamic* number and position of objects (theoretical password space may dynamically change); *observability* (e.g., subtle vs obvious interaction); user-specific *features of interaction* such as, e.g., speed or hold time.

Desk Setup

For investigating our concept, we chose a desk setup. This choice is motivated by two factors. It is 1) of manageable size and, hence, easily controllable in a lab setup. At the same time, it is 2) of high relevance as authentication at their desk is part of the daily business for many users.

The desk setup for our study is motivated by an analysis of photos ($N = 107$) that users published in an online forum (refer to Tab. 1 for the results).

Prototype

We built a first prototype of *Interact2Authenticate* (cf. Fig. 2). By means of capacitive touch sensors, foil (in case an object's surface is not conducting by itself, cf. Fig. 3), and a Raspberry Pi, we can recognise touches on specific points at connected objects. We attached our prototype to a desk setup (cf. Fig. 1). We implemented a simple GUI which al-

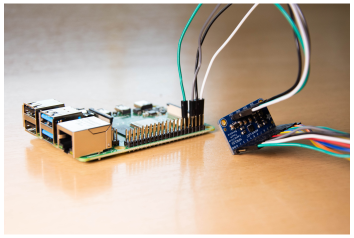

Figure 2: *Interact2Authenticate* prototype: A Rasperry Pi connected to capacitive touch sensors.

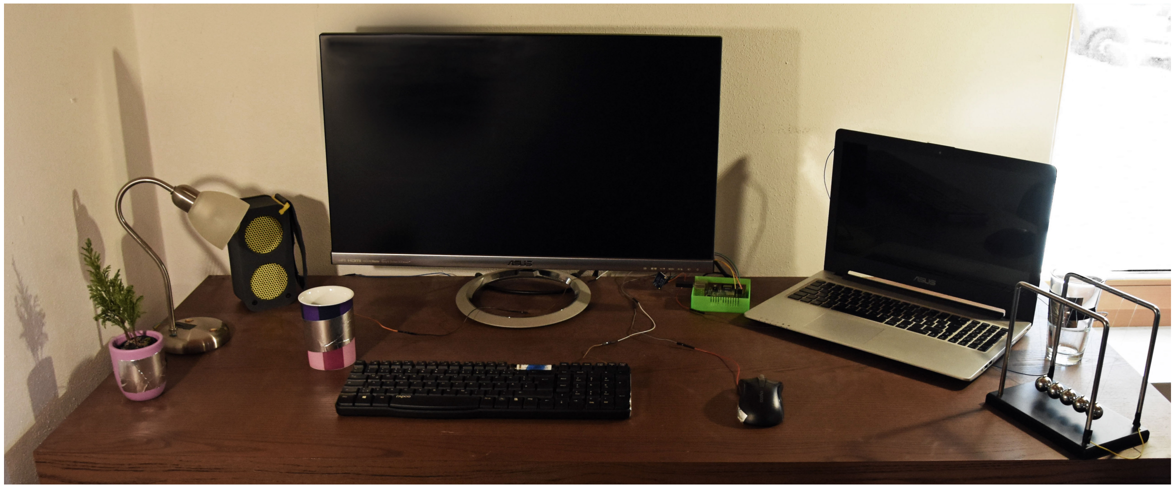

Figure 1: Desk setup with *Interact2Authenticate*: We integrated our prototype (in a green, 3D printed case) to a desk setup for a preliminary usability study. The setup is based on our findings from Table 1.

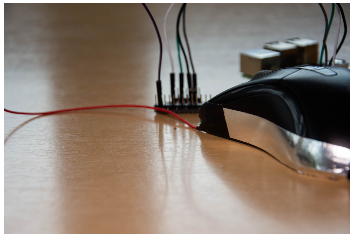

Figure 3: Workaround: Adding additional foil to non-conducting surfaces to recognise touch input by means of capacitive sensors.

lows users to enter a conventional, text-based password as well as an authentication secret based on *Interact2Authenticate*.

Preliminary Results

In an exploratory study ($N = 18$) on the usability of our concept, we compared *Interact2Authenticate* with a conventional, text-based password. We employed the (un)changed desk setup as between-subjects independent variable (i.e., we changed the desk setup within the study session for half of the participants).

Participants. We recruited 18 participants, 9 female. Four participants were students, others working in a full time job. Participants ATI scale [3] ranged from 2.11 to 6 (where 6 is the highest possible score, referring to high technical affinity), with an average of 4.28.

Results. We found that participants' workload was similar for the textual password as well as our novel mechanism using the NASA-TLX questionnaire [6] (*Interact2Authenticate*: 28.5; textual password: 27.6). The system usability scale (SUS) for *Interact2Authenticate* was 83 on average, where 100 is the highest possible score (i.e., highest usability). Participants further rated *Interact2Authenticate* to be rather secure (mean 5.1 on a 7-point Likert scale).

Open Questions & Future Research

Password Spaces

The theoretical password space for *Interact2Authenticate* is huge. Imagine the concept was built natively into smart environments, it would comprise unlimited objects and distinct touch points. Additionally, users' unique input features such as hold time, input speed, and grip might be applied as biometric features. However, we are still missing knowledge on potential “sweet spots” that may result from participants’ password creation.

Application Areas

While we for now suggested *Interact2Authenticate* as an authentication mechanism for desk setups, we imagine further application areas. This may not only comprise authentication in various settings (e.g., smart homes, offices), but also further use cases such as data collection in smart homes to, e.g., support research purposes or to foster automation within the home. *Interact2Authenticate* could also serve as a novel input modality, i.e. for explicit commands rather than authentication.

Challenges

We still see open challenges in the current version of *Interact2Authenticate*. Our preliminary prototype was bound to cables and conductive surfaces. We needed to add additional foil in case an object came with a non-conductive surface (cf. Fig. 3). Seamless integration of *Interact2Authenticate* needs further iterations of our prototype. Further, to avoid the aforementioned “sweet spots”, means to nudge users to choose usable and secure authentication secrets might need to be found.

Conclusion

In this position paper, we presented *Interact2Authenticate* as a novel authentication mechanism for smart environments that blends with users’ daily interaction. We present and discuss early insights from our first prototype. From our preliminary study, we learned that users generally appreciated our concept and idea, perceiving it to be usable as well as secure.

We are looking forward to discuss the strengths and weaknesses of *Interact2Authenticate* at the CHI 2020 workshop on *Authentication Beyond Desktop and Smartphones*.

Acknowledgements

We thank Elias Amort for ideating, implementing and evaluating the first version of *Interact2Authenticate*. We further thank Sarah Delgado Rodriguez and Lukas Mecke for their valuable contribution throughout the project as well as their help in data analysis.

REFERENCES

[1] F. A. Alsulaiman and A. El Saddik. 2008. Three-Dimensional Password for More Secure Authentication. *IEEE Transactions on Instrumentation and Measurement* 57, 9 (Sep. 2008), 1929–1938. DOI:http://dx.doi.org/10.1109/TIM.2008.919905

[2] Florian Alt and Emanuel von Zezschwitz. 2019. Emerging Trends in Usable Security and Privacy. *Journal of Interactive Media (icom)* 18, 3 (Dec. 2019). DOI:http://dx.doi.org/10.1515/icom-2019-0019

[3] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human-Computer Interaction* 35, 6 (2019), 456–467. DOI: http://dx.doi.org/10.1080/10447318.2018.1456150

[4] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, and Pranjal Rathod. 2013. Secure authentication with 3D password. (2013).

[5] 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.

[6] NASA. 1980. NASA-TLX Workload Index. (1980). https://humansystems.arc.nasa.gov/groups/TLX/downloads/TLXScale.pdf (Accessed January 2020).

[7] S. Prange, E. von Zezschwitz, and F. 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. DOI: http://dx.doi.org/10.1109/EuroSPW.2019.00024