Act2Auth – A Novel Authentication Concept based on Embedded Tangible Interaction at Desks

Sarah Delgado Rodriguez*
sarah.delgado@unibw.de
University of the Bundeswehr Munich
Munich, Germany

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

Lukas Mecke
University of the Bundeswehr Munich
Munich, Germany
lukas.mecke@unibw.de

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

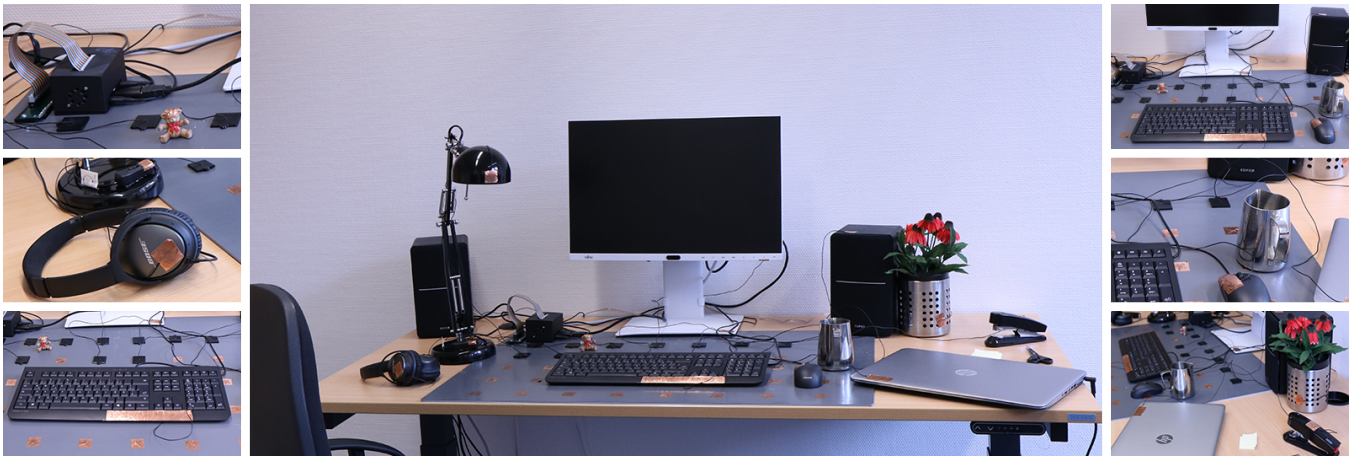


Figure 1: *Act2Auth* embeds authentication in the way in which users interact at a desk setup. Users of *Act2Auth* can authenticate by touching objects or the desk itself in a secret order similar to a password. To evaluate our concept, we built a prototype that applies capacitive sensing to daily life objects and conducted an exploratory user study ($N = 8$).

ABSTRACT

Authentication (e.g., entering a password) is frequently perceived as an annoying obstacle when interacting with computational devices, but still essential to protect sensitive data from unauthorized access. We present *Act2Auth*, a novel concept for embedding authentication into users' established routines by sensing tangible interactions at desks. With *Act2Auth*, users can authenticate by performing (secret) routines, such as putting a cup on their desk, rearranging their keyboard, and touching their mouse. The *Act2Auth* concept is informed by (1) an object analysis of 107 desk photos from Reddit, (2) an online survey ($N = 65$) investigating users' strategies for creating touch-based authentication secrets, and (3) a technical exploration of capacitive touch-sensing at desks. We then (4) implemented a prototype and evaluated the usability as well as the memorability of *Act2Auth* compared to textual passwords ($N = 8$). With *Act2Auth*, we provide fundamental work on how to embed authentication tasks into our daily tangible interactions.

CCS CONCEPTS

• **Human-centered computing** → **Interactive systems and tools**; • **Security and privacy** → *Usability in security and privacy*.

KEYWORDS

tangible authentication, tangible security, embedded authentication, capacitive sensing

ACM Reference Format:
Sarah Delgado Rodriguez, Sarah Prange, Lukas Mecke, and Florian Alt. 2024. *Act2Auth* – A Novel Authentication Concept based on Embedded Tangible Interaction at Desks. In *Eighteenth International Conference on Tangible, Embedded, and Embodied Interaction (TEI '24), February 11–14, 2024, Cork, Ireland*. ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3623509.3633360

*Both authors contributed equally to this research.

TEI '24, February 11–14, 2024, Cork, Ireland

ACM ISBN 979-8-4007-0402-4/24/02…$15.00
https://doi.org/10.1145/3623509.3633360

1 INTRODUCTION

Today, many tasks performed on a desk entail using a computational device (e.g., a PC, notebook, or tablet). Such tasks include work-related activities, but also leisure activities like gaming, online shopping, or social media. Many of those tasks require access to or the use of sensitive data, such as customer data, personal accounts (e.g., e-mail, banking, or social media accounts), or private files. This data is oftentimes protected by an authentication mechanism. As a result, users cannot directly proceed to their primary task but first need to authenticate, for example, by entering a text-based password or scanning their fingerprint. This creates a challenge: authentication is usually a secondary task [57], creating an inconvenient barrier to the intended use. While authentication is necessary to protect sensitive data from unauthorized access, users frequently perceive it as annoying and interrupting, especially since it is required multiple times a day [2, 21] (e.g., for accessing different accounts). Moreover, the ever-increasing number of required passwords exceeds users' memorability, leading to passwords being reused or noted down [2]. At the same time, related work on embedded interactions proposes leveraging the way in which users interact with everyday objects as a means for user input [44, 61, 63]. This enables interactions with the digital world in a way that seamlessly blends with users' established routines and physical environments. Various approaches to enable sensing of tangible interactions with everyday objects exist. For example, capacitive sensing [47, 48], near-field communication [18], or acoustic sensing [44] can be leveraged for this purpose. Moreover, an ever-increasing number of smart objects can detect when they are being touched (e.g., touch-sensitive light switches, lamps, headphones).

In this paper, we explore the potential of such embedded interactions for user authentication. More specifically, we propose *Act2Auth*, a concept leveraging embedded tangible interactions for authentication at desks, to increase usability and reduce memory burden. Users of *Act2Auth* authenticate by the (secret) order in which they interact with objects on their desks. For instance, an authentication secret could consist of grasping their desk to pull their chair up, opening their laptop, and placing their keyboard in front of them. This allows for authentication to blend with the way in which users naturally interact with a desk setup. Additionally, our approach can potentially reduce memorability issues common for authentication mechanisms, as motor and visual memory can be leveraged. By focusing on users' desks which is where they often authenticate to, for example, unlock their PCs, we also provide a meaningful context for *Act2Auth*. We expect that this further supports memorability by supporting mnemonics [52, 64].

To inform *Act2Auth*, we investigated the challenges of using tangible interactions with daily life objects at desks for authentication. First, we investigated people's typical desk setups and how they might create touch-based authentication secrets in such an environment. Next, we technically explored capacitive touch-sensing at a desk. The insights from these explorations informed the *Act2Auth* concept. *Act2Auth* senses tangible interactions with stationary (e.g., a desktop PC or plant pot) and dynamic (i.e., movable like a cup or the mouse) daily life objects at desks in a privacy-preserving and unobtrusive manner. *Act2Auth* enables secret-based authentication (i.e., users perform a secret input pattern) which can be embedded into users' established routines. We then implemented a prototype, allowing us to explore *Act2Auth* in a user study ($N = 8$) and compare it to text-based passwords. In this study, we evaluated the usability of creating and inputting *Act2Auth* secrets as well as their memorability. Participants rated *Act2Auth* to be very usable and created secrets that they considered secure. They integrated secrets into their interaction routine (e.g., ending at the mouse), created stories around them, and tried to leverage motor memory.

Our work provides an important step-stone for embedding novel tangible authentication mechanisms with users' established routines and environments to increase both, usability and security. We envision our concept to be applied in the future to additional objects in a variety of environments.

Contribution Statement. Our contribution is two-fold: 1) We present the *Act2Auth* concept, leveraging tangible interaction at desks for authentication. We extensively studied the application environment, secret creation, and technical feasibility to inform the concept. 2) We present a real-world prototype and use it in a lab study to assess usability and memorability while creating and inputting secrets using *Act2Auth*.

2 BACKGROUND & RELATED WORK

We draw from several strands of related work. After providing a brief introduction to authentication, we look into how tangible interaction can be leveraged for authentication in various ways. For our implementation, we illustrate how everyday objects can be enhanced for tangible interactions.

2.1 Introduction to Authentication

Authentication mechanisms can generally be classified into knowledge-based, token-based, and biometric schemes [43].

Many users are familiar with *knowledge-based* mechanisms such as textual passwords, PINs, or graphical patterns. One important measure to assess the security of any knowledge-based authentication mechanism is the size of its *password space*, i.e. the set of all distinct authentication secrets that can be created for the respective mechanism. For instance, consider a 4-digit PIN: the number of all possible combinations is 10.000. The larger the password space of a mechanism, the more difficult it is for an attacker to *guess* a secret. However, as users are confronted with an increasing number of such secrets (e.g., for various accounts), their *memory* reaches its limits. To address this, prior work proposed mechanisms leveraging motor memory [13, 38, 40, 50, 59, 66]. Moreover, secrets are prone to being *observed* by attackers while being entered.

Tokens do not pose any requirements to cognition, but need to be carried by users for authentication (e.g., smart cards for doors) and, hence, can be forgotten, lost or stolen.

Biometric schemes leverage users' unique characteristics for authentication. Popular examples are fingerprint scans or face recognition on modern smartphones. While these mechanisms are fast and easy to use, they cannot (easily) be changed and may not work well under certain conditions (e.g., face recognition in darkness, wet fingerprints [6]). Generally, the aforementioned mechanisms are used for so-called *explicit* authentication, i.e., users are required to consciously perform the authentication task.

A different approach is to embed authentication with other tasks and/or users' environments, namely *implicit* authentication [35]. Examples include but are not limited to, authentication based on users' unique typing behavior [30–32], mouse movements [25, 30], gait [22], or eye movements [36]. As such, authentication runs in the background and is performed during users' actual interaction. However, the functionality of implicit authentication systems is difficult to understand for users, in particular when authentication fails. Hence, related work observed trust and usability issues [8, 27].

In our work, we propose a new scheme that we deliberately designed as a knowledge-based mechanism: users remember a series of embedded interactions and perform an explicit authentication task. At the same time, the mechanism could additionally consider biometric features for authentication, such as the time between interacting with two objects, or the exact way of grabbing a certain object, thus providing a second layer of security.

2.2 Leveraging Tangible Interaction for Authentication

Authentication mechanisms based on tangible user input can improve the memorability of authentication secrets since they leverage motor memory [13, 38, 40, 59]. Hence, related work proposes novel tangible user interfaces, as well as interaction with everyday objects or fully embedded approaches for authentication.

2.2.1 Tangible User Interfaces for Authentication. Related work suggested several novel, dedicated tangible user interfaces for authentication. *3D-Auth* consists of 3D-printed objects that users manipulate (e.g., rotate) in a secret manner and place them on a touchscreen [38]. Other approaches are based on manipulating a *Rubiks cube* [4, 40]. Users of *Bend Passwords* can authenticate by bending a flexible sheet in a secret manner [37]. However, similar to traditional authentication tokens (e.g., keys or smartcards), such dedicated tangibles can be lost, forgotten, or stolen.

2.2.2 Authentication Through Interaction with Objects and Environments. Related work also suggested augmenting everyday objects (e.g., door handles) with sensing capabilities to assess usage patterns for authentication [10, 15, 19, 20, 65]. Similarly, sensor-enhanced wristbands or smart watches can be used to authenticate users when touching or moving specific objects [34, 65, 67]. Furthermore, related work presents authentication mechanisms for virtual environments where a secret can consist of multiple objects in a 3D environment that a user can interact with [3, 16, 29].

Related work also proposes authentication mechanisms to be fully embedded into other tasks or into users' physical environments. Krašovec et al. [30] leverage users' behavior in a room while interacting with a desktop PC and conducting everyday tasks for authentication. They measure how their participants use a mouse and keyboard, as well as the used resources of the PC. Moreover, they capture the user's movement patterns inside the room.

Other researchers suggested attaching inertial sensors to movable everyday objects (e.g., cabinet doors, drawers, or remote controls), basing authentication on unique movement patterns [20, 65].

Further examples include mechanisms that measure users' unique interaction patterns with computational devices, such as their typing behaviour [5, 31, 68], mouse [26, 45], touch [1, 23], gait [41, 42] or eye-movement patterns [28, 51, 69].

2.3 Enhancing Everyday Objects to Sense Tangible Interaction

Enhancing everyday objects with sensing capabilities (e.g., by prototyping novel sensing approaches [10, 17, 44] or retrofitting commercial on-object sensors like the MetaSensor[1] or the SmartThings Multipurpose Sensor[2]) offers opportunities for novel interactive applications [10, 17, 20, 46, 65]. Prior work used capacitive sensing [17], inertial measurements [19, 20, 65], acoustic sensing [44], NFC [18] or multi-sensor-approaches [10, 46] to measure tangible interactions with everyday objects. Looking at tangible interactions specific to desk/table environments, related work presented tabletop interfaces to be used in conjunction with everyday objects like paper, domino bricks, figurines, or model cars [33, 54, 60]. Such interfaces usually track the position of the objects on the table or desk and the user's tangible interactions with them using optical-based tracking [12, 24], capacitive sensing [49, 55, 56], or NFC [54].

2.4 Summary & Distinction of *Act2Auth*

Related work leverages tangible interactions with *multiple* physical everyday objects for *implicit* authentication (e.g., [65], [20] or [30]). Such mechanisms allow embedding authentication in users' natural tangible interactions with their environment, instead of having to perform complex or unnatural gestures with single objects (e.g., shaking [14]). However, purely implicit mechanisms suffer from a lack of trust and usability [8, 27].

With *Act2Auth*, we instead embed knowledge-based authentication into routine tangible interactions with everyday objects at desks. Thus, users are in control of the authentication process since they can *explicitly* choose the timing of the authentication and the authentication secret. With *Act2Auth*, we leverage the advantages of both, traditional explicit and implicit authentication. Inspired by implicit authentication mechanisms, our system supports non-intrusive or *calm* [58] authentication and reduces users' effort required for authentication by embedding authentication into routines and environments. In contrast, with other explicit authentication mechanisms, users are required to perform a specific additional authentication interaction (e.g., entering a password or scanning a fingerprint), usually on a designated device.

Moreover, *Act2Auth* provides a customizable password space, which is composed of all objects situated on the user's desk. With our system, we specifically embed authentication in a meaningful environment for authentication, which is desks. As such, the *Act2Auth* authentication procedure cannot only be used for unlocking the main device (e.g., laptop or PC) but also for accessing particular functionality such as e-mail or other software. *Act2Auth* supports memorability of authentication secrets by leveraging motor memory and mnemonics [50, 66], since involved objects may already carry a certain metaphor.

[1] https://metasensor.com/, last accessed July 31, 2023
[2] https://www.samsung.com/de/smartthings/sensor/smartthings-multipurpose-sensor-gp-u999sjvlaea/, last accessed July 19, 2023

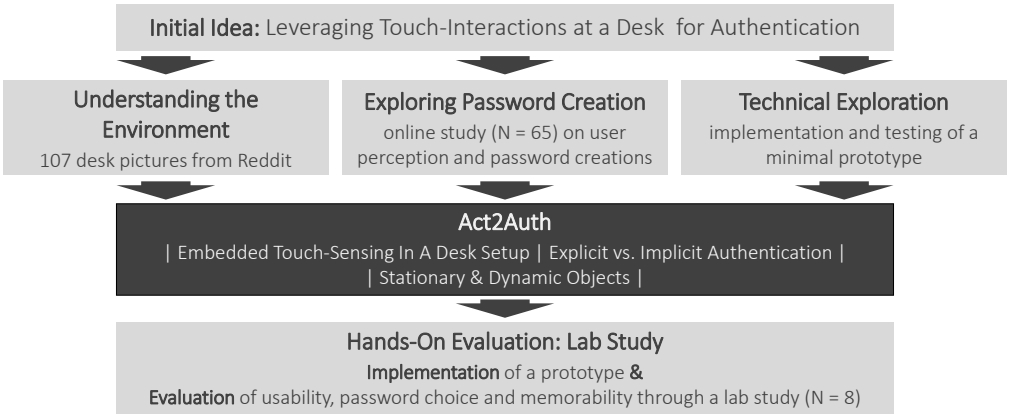


Figure 2: We derived *Act2Auth* based on a three-step exploration of the application environment (i.e., the user's desks), secret creation, and a technical exploration. Based on our concept, we developed a prototype that we used for a final evaluation.

3 RESEARCH APPROACH

In this work, we leverage touch interactions at desks for embedded authentication (cf. Figure 2). In particular, we first explored the application environment in detail, along with a first technical implementation. To this end, we (1) analyzed desk pictures (N = 107) that users posted in the online forum Reddit; (2) built an online study, using a photo of a desk setup, to investigate how users would perceive such a mechanism and create authentication secrets; and (3) implemented an initial prototype in a desk environment and informally tested technical feasibility. Next, we derived the *Act2Auth* concept, based on our findings of these initial explorations. We then built a prototype, which allowed us to conduct an initial user study, comparing *Act2Auth* secrets with text-based passwords. The aim of this study was to evaluate the usability, memorability, and secret choice of both authentication mechanisms.

4 UNDERSTANDING DESK SETUPS, POTENTIAL AUTHENTICATION SECRETS, AND TECHNICAL FEASIBILITY

4.1 Understanding Desk Setups

As a first step, we analyzed desk pictures that users posted on the online forum Reddit. In particular, we collected N = 107 pictures posted on the subreddits *r/workspaces*[3] and *r/desksetup*[4] until January 8, 2021. The descriptions of both subreddits indicate that these forums are specifically intended to be used to "share [users'] desk setups". We used these pictures to identify objects that are common on peoples' desks. We found that more than 20% of the pictures showed a mouse, a keyboard, a display, a laptop or tablet, headphones, decorative objects, speakers, plants, lamps, or a desktop PC. Appendix A provides details on how many pictures showed each of these objects. These findings inform the desk setup used for our subsequently conducted online and lab studies.

In particular, we learned that *stationary* (e.g., displays, lamps, or desktop PCs) and *dynamic objects* (e.g., mouse or headphones) should be considered for *Act2Auth*. Note that it is possible that the analyzed photos showed specifically prepared setups rather than real desk setups. Thus, we corroborated our findings by also inquiring about participants' desks in our online survey (cf. Section 4.2.6).

4.2 Secret Creation: An Online Survey

Next, to explore how people would create authentication secrets using *Act2Auth*, we conducted an online survey (N=65).

4.2.1 Apparatus. For the online survey, we took a picture of a desk with objects based on Section 4.1: laptop, external monitor, keyboard, mouse, headphones, speakers, lamp, office utensils, and decoration. We additionally added a coffee cup as a dynamic, movable object (see Figure 3). We used this photo as the basis for a click-prototype (i.e., participants could compose *Act2Auth* secrets by clicking on certain positions in the photo).

4.2.2 Survey Structure & Questions. The online survey consisted of five parts[5]: 1) We explained our research and the data collection, and gathered participants' consent; 2) We gave more details on the concept and participants tried our click-prototype; 3) Participants created three *Act2Auth* secrets (one they considered to be weak, one medium, and one strong in randomized order) and we asked them about their choice; 4) We asked about participants' demographics, including their desk; 5) We put final questions on our concept and comparison to conventional mechanisms.

4.2.3 Participants. We recruited 70 participants through university mailing lists and social networks (cf. Table 1 for demographics). We excluded 5 participants due to missing click data. Of the remaining 65 participants, 40 were female, and 24 were male. Most participants were right-handed, students and spend up to 12 hours at their desks at work as well as up to 8 hours at their desks at home. Some participants used desks exclusively (i.e., either at work or at home).

[3]https://www.reddit.com/r/workspace/, last accessed in August 2023
[4]https://www.reddit.com/r/desksetup/, last accessed in August 2023

[5]We provide details, including the full list of questions, in Appendix B.

Table 1: Online Survey: Participant demographics, employment status, and desk time.

	Demographics	
Age	Mean	26.91
	SD	8.84
Gender	male	24
	female	40
	prefer not to say	1
Hand	Right	57
	Left	8

Employment Status	
student	40
employed full time	19
employed part-time	3
other	2
retired	1

	Desk Hours	
At Work	Mean	5.55
	SD	2.79
	Min	0
	Max	12
At Home	Mean	2.51
	SD	1.92
	Min	0
	Max	8

4.2.4 Ethical Considerations. Low-risk studies like this online survey are exempt from formal approval by an IRB at our institution and local regulations. Nevertheless, we implemented the online survey based on best practices provided by our institutional ethics board and local data protection regulations. In particular, participants were first informed about the study, the applied data collection, and their corresponding rights. We then asked them to consent to the participation and data collection, prior to collecting any data. Data was stored anonymously on university servers.

4.2.5 Limitations. Our survey has some limitations. We tested a spatial concept on a 2D photo. This may have made it more difficult for participants to define and enter a secret. Hence, we do not report any interaction times but focus on chosen objects. Further, our sample is biased toward young students (mean age: 27). However, all participants stated to spend at least some time at a desk (cf. Table 1) and thus represent our target group.

4.2.6 Results. Our analysis consists of 1) characteristics of secrets (length, objects) and 2) a thematic analysis [7] of participants' answers to open-ended questions. We refer to participants with IDs as assigned by our survey tool.

Desk Setups. We asked participants to describe their own desk by selecting which of our provided objects are on their desk (they could mention more) and which they would use for *Act2Auth* (cf. Table 2 for an overview). Participants mentioned having *stationary* objects as well as personal, potentially *changing* items on their desks. P558 reported not having a desk. P485 and P577 reported on dynamic desk setups (e.g., using a portable device at various tables; a dynamic office environment with changing desks).

Chosen Secrets. Participants set a weak, medium, and strong *Act2Auth* secret each (195 in total). They considered their secrets usable and increasingly secure (cf. Table 3). In particular, they chose secrets of increasing length for weak (Mean=2.62, SD=1.54), medium (Mean=4.52, SD=1.80), and strong (Mean=7.26, SD=4.05).

Objects. We predefined areas in the photo showing concrete *objects*. Clicks to other areas were counted as *background* (cf. Figure 3)). Most clicked were the keyboard (292), background (mostly the table, 178), lamp (174), and monitor (162).

Considerations. Participants motivated their secret choice by multiple factors, mainly related to the *position* and *characteristics* of objects. For the position, participants mentioned proximity to their dominant hand, objects in reach and/or in view, actively mixing close and far objects in one secret, or involving the whole desk. Objects' characteristics included *stationary* vs *dynamic* objects and the possibility to have *multiple touchpoints* per object (e.g., from multiple sides). Some participants also considered *memorability* for their choice (e.g., choosing simple secret combinations or involving their usual desk routine). P591 described a story involving the objects to ease memorability.

Properties. Participants mentioned usability properties such as: easy to *remember*, *fast* input, objects *in reach*, and choosing *patterns*. From a security perspective, participants mentioned *increased length*, *multiple touchpoints* per object, using *specific touchpoints* (rather than the object as a whole), and spreading their secret over the desk (e.g., involving the whole desk and/or including far away objects). Others included unusual objects to avoid guessing or made an effort to be subtle in their input to reduce the odds that their secret could be observed. P591 even took measures to assess security: *"zxcvbn*[6] *tells me an offline brute force attack with 10k guesses a second will take 3 years."*

Table 2: Online Survey (N = 65): Objects that participants have on their (most used) desks as well as objects they would involve for *Act2Auth*. Items in the lower part were no predefined answers but were given by the participants.

Device/Object	x of 65	%	Use for *Act2Auth*	%
laptop/tablet	46	71%	18	28%
mouse	43	66%	14	22%
display	40	62%	16	25%
keyboard	39	60%	21	32%
lamp	35	54%	12	18%
decoration	34	52%	8	12%
headphones	29	45%	0	0%
speaker	14	22%	3	5%
plant	13	20%	3	5%
office supplies	49	75%	12	18%
beverage	11	17%	2	3%
books	8	12%	5	8%
telephone	6	9%	4	6%

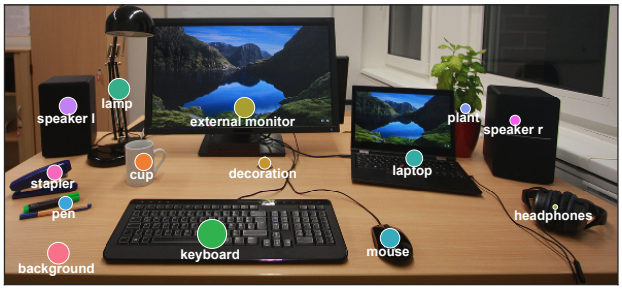


Figure 3: Distribution of clicked-on objects in our online survey. Larger bubbles indicate that the respective object was selected more often. Clicks outside object boundaries were assigned to 'background'

[6]password strength estimation, https://github.com/dropbox/zxcvbn, last accessed in August 2023

Table 3: Online Survey: Assessment of usability and potential threats for *Act2Auth* on a 5-point Likert scale (5=strongly agree). The table shows median values as well as the number of "I can't tell"-answers in brackets.

Usability Items	weak	medium	strong
Entering the secret was fast.	5	4	3
Entering the secret was easy.	5	4	3
The entered secret is secure.	1 (2)	3 (2)	4 (1)
I can easily remember the secret.	5	4	3
The following person can enter my secret correctly.	**weak**	**medium**	**strong**
Somebody who observed my input.	5 (1)	5 (1)	4 (1)
Somebody who knows me well and guesses the secret.	4	2 (1)	2
A stranger who guesses the secret.	4 (3)	2 (1)	1

Table 4: Online Survey: Comparison of *Act2Auth* to conventional mechanisms on a 5-point Likert scale (5=strongly agree). The table shows median values as well as the number of "I can't tell"-answers in brackets.

	pin	pattern	password	fingerprint	face	TAN
I would use *Act2Auth* rather than:	2 (0)	3 (0)	2 (1)	1 (2)	2 (1)	2 (4)

Potential Threats. We asked participants to assess potential threats (i.e., the risk of *Act2Auth* secrets being guessed/observed). Overall, participants considered the weak secret more likely to be guessed or observed (cf. Table 3 for details).

Comparison & Concerns. Participants often preferred mechanisms they were used to (cf. Table 4). Some mentioned explicit concerns, e.g. desk settings that are dynamic (e.g., *"I'd be worried what would happen if my colleague borrowed my pen"*, P571). Others raised privacy concerns about a camera that might be included in the implementation of *Act2Auth* to recognize input (P577, P606). P608 was concerned regarding entropy, stating that the entropy for textual passwords is higher. P598 mentioned that traces of use visible in the dust on their desk might support attackers.

4.3 Technical Exploration

Next, we built an initial prototype to explore and understand the opportunities and challenges of integrating touch-sensing capabilities in desk environments. For this purpose, we used a Raspberry Pi 4 Model B[7] and Adafruit's MPR121[8] capacitive touch shield2 as shown in Figure 4a. The MPR121 provides 12 pins for self-capacitive touch detection. We then created a typical desk setup including the same 11 objects included in the online survey (cf. Figure 4b). All objects were augmented with a conductive surface by sticking aluminum foil to them. Each foil was wired to the MPR121 capacitive touch sensor shield (cf. Figure 4c). The sensor was also connected to the Raspberry Pi. The Raspberry Pi logged and visualized users' touch interactions (timestamps) with the augmented objects.

[7]https://www.raspberrypi.org/products/raspberry-pi-4-model-b, last accessed July 31, 2023

[8]https://www.sparkfun.com/datasheets/Components/MPR121.pdf, last accessed July 31, 2023

4.4 Lessons Learnt

From both, the online survey and technical exploration, we derived further requirements for *Act2Auth*. In particular, we found that participants were reluctant towards cameras at their desks (P577 and P606). Hence, less privacy intrusive sensing technologies such as capacitive sensing would be more appropriate. However, additional cables on the desk (as in Figure 4) could interfere with users' interaction routines. Furthermore, *Act2Auth* should incorporate sensing capabilities to distinguish touches on the desk itself as a considerable number of clicks in the online survey was placed on the "background" of our photo (i.e., mostly the desk). Moreover, as we found varying desk setups and participants in the online survey chose objects of several types, *Act2Auth* should be easy to personalize to include both, objects that are stationary on a desk and objects that are movable and/or personal for individual users. Lastly, the prototype should not feel like yet another device being added to the desk but rather be tightly integrated into the environment.

5 THE *ACT2AUTH* CONCEPT

The idea behind *Act2Auth* is to leverage *touch-interactions with daily life objects at desks* for seamless, embedded authentication. We detail the concept in the following.

5.1 Embedded Touch-Sensing At Desks

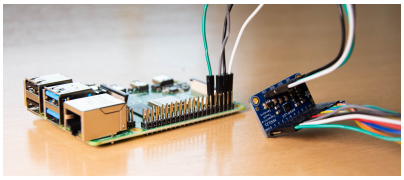
Act2Auth uses embedded touch-sensing based on capacitive sensing. We deliberately do not use cameras to detect interactions, to protect users' privacy. Instead, *Act2Auth* senses touch on objects and on the desk itself. It is also unobtrusively integrated into the desk setup instead of relying on additional objects or tokens. Thus, it does not interfere with the positioning of other objects or routines.

5.2 Interaction with Static vs. Dynamic Objects

Act2Auth allows for authentication by touching *stationary* and *dynamic* objects at desks. As such, an *Act2Auth* secret can comprise touching or moving objects that are permanently present on the desk, or interact with objects that only come into play temporarily. This has implications for both, the usability and security of the authentication procedure. Thinking about memorizing an *Act2Auth* secret, movable or dynamic objects might pose a challenge and be harder to remember if currently at a different position. Considering a potential attacker who might try to guess an *Act2Auth* secret, movable objects might make it more difficult as users put them in locations where attackers do not expect them.

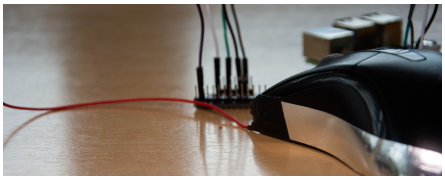
5.3 Embedding Authentication into Interaction Routines at Desks

Act2Auth allows users to authenticate by touching an arbitrary sequence of objects. Also moving objects can be part of a secret. Furthermore, multiple touches per object or even "knock patterns" on a single object could be used. In addition, the overall length of the *Act2Auth* secret can be varied to increase the security of the secret and hinder illegitimate entities from guessing it. While an increasing number of knowledge-based secrets (e.g., for different accounts or functionalities) might exceed users' memory limit, we believe that *Act2Auth* can leverage motor memory [50] or foster



(a) The controlling circuits of the initial prototype, including one Raspberry Pi 4 and one MPR121 capacitive touch shield.

(b) Desk setup of the initial prototype, including objects that can be typically found on a desk.



(c) The MPR121 shield can be connected via wires to up to 12 conductive surfaces and subsequently sense touches on those.

Figure 4: Technical Exploration: These photos illustrate the initial prototype that we used for a first exploration of how to embed touch sensing capabilities in a desk setup.

the use of mnemonics [66]. Another strength of *Act2Auth* is that authentication can blend with users' interaction routines at desks, and that objects being part of the secret may carry a certain metaphor by default. This allows to integrate the authentication procedure seamlessly with the way in which users interact at their desks.

6 IMPLEMENTATION AND EVALUATION

6.1 Implementation of the Prototype

To allow for a hands-on user evaluation of *Act2Auth*, we build a desk pad prototype. The prototype consists of an active control unit in the form of a Raspberry Pi 4 Model B with four MPR121 capacitive sensor shields and a desk pad that includes 40 copper electrodes on its surface (cf. Figure 1). This enables self-capacitive sensing directly on the electrodes or on other conductive surfaces that are in contact with an electrode. To enable touch sensing on other objects we developed reusable connectors. Those can be connected to an electrode to create a wired bridge to any object and are attached with copper tape. The connectors, thus, enable touch sensing on almost any object and solid surface. For further details on the implementation, please refer to our previously published late-breaking work [11]. In summary, our prototype allows for self-capacitive touch sensing on 1) the pad itself (cf. Figure 6), 2) conductive movable or stationary objects that are in contact, and 3) objects or surfaces wired to the prototype with reusable connectors.

6.2 Evaluating *Act2Auth*: A Lab Study

In a lab study, we compared *Act2Auth* secret with text passwords. We chose text passwords as a baseline since they are among the most widely used considering a PC/laptop at a desk. The main goal of this study was to understand users' strategies for creating and memorizing secrets.

6.2.1 Apparatus. We set the *Act2Auth* prototype up in an office at our institute (this office was solely used for that purpose). We connected headphones, a desk lamp, speakers, decorations, a monitor, a plant, office supplies, a laptop, a mouse, a keyboard, decoration, and a coffee cup to our prototype as potential touch input. Additional touchpoints on the desk pad itself were also available (cf. Figure 6).

6.2.2 Study Design. We investigated *password creation strategies*, *secret input* (unobserved and observed) as well as *memorability* (cf. Figure 5 for an overview). We introduced AECRET STRENGTH as a within-subjects variable with two levels (*semi*-secure, *very* secure). For every level of strength, participants created two SECRET TYPES: one *text password* (baseline) and one *Act2Auth* secret. We chose generic descriptions for the secret strength level[9], as data sensitivity is highly subjective. We counterbalanced SECRET STRENGTH and SECRET TYPE according to a Latin Square [62]. We asked participants in each condition to *create* a secret that they would use and be able to memorize. The chosen secret needed to be entered twice under varying INPUT conditions (in counterbalanced order): once while being alone in the office (i.e., *unobserved*) and once while somebody else was present and might *observe* their input[10]. Finally, to measure short-term memorability, we asked participants to enter all created secrets again at the end of the session.

6.2.3 Recruitment & Procedure. We recruited 8 participants through university mailing lists and social networks. Participants were reimbursed with € 5. Each study session took 30 minutes and was audio and video recorded. The detailed procedure was as follows[11]:

(1) We introduced participants to our concept and gathered their consent. They then tried out interacting with our prototype.
(2) Participants created a secret and confirmed it (similar to a usual set and approve process). We added a short questionnaire and asked for strategies.
(3) Participants then entered the secret twice (OBSERVED and UNOBSERVED) and answered Likert items for each. We again asked about their strategies[12].
(4) We finalized the study with demographic questions and a semi-structured interview on the concept.
(5) Participants had to enter all their secrets again in the order of creation to capture short-term memorability.
(6) Participants were reimbursed and could ask questions or provide feedback.

6.2.4 Ethical Considerations. With our study, we followed any recommendations given by our institutions' ethics boards. In particular, we made sure to gather participants' informed consent by providing them with information on the study procedure and goal, the data collection, processing, and storage, as well as on their rights of withdrawal and further legal rights.

[9] Full descriptions are available in Appendix C.
[10] Note that we did not specify any explicit actions the observer might take.
[11] We provide details, including the full list of questions, in Appendix C.
[12] Steps 2-3) were repeated in counterbalanced order for each SECRET TYPE and SECRET STRENGTH (cf. Figure 5).

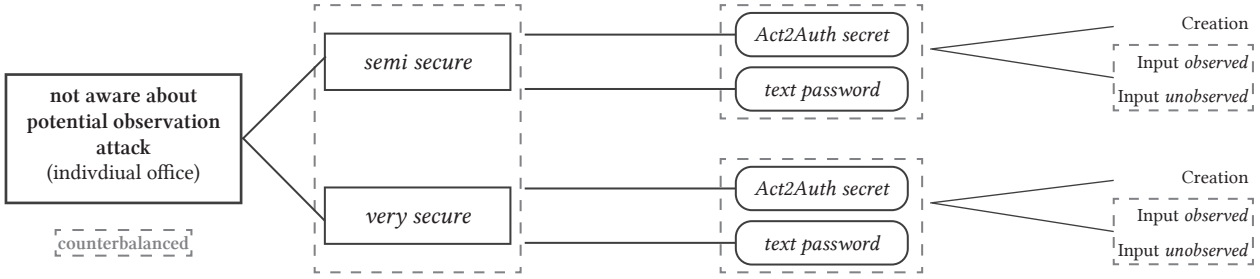


Figure 5: *Act2Auth* Lab Study Design: We conducted a within-subjects study with Secret Strength (semi-secure, very secure), Secret Type (*Act2Auth* secret, text password) and Input (observed, unobserved) as independent variables. We counterbalanced the input within type, and type within strength, respectively.

Table 5: Length of secrets and Levenshtein distance (i.e. number of alterations) between chosen and memorized secrets.

	Levenshtein distance	secret length mean	min	max
Act2Auth secret semi	0.571	7.125	3	17
Act2Auth secret very	2.286	11.250	5	39
text password semi	0.000	10.125	5	15
text password very	1.875	16.250	8	30

The collected data were anonymized and stored on university servers. Audio recordings were only stored until being transcribed and videos were deleted after analyzing participants' interactions and behavior. For the text password condition, we explicitly told them to not use any passwords they use in real life and analyzed metadata only (e.g., length).

6.2.5 Participants. Participants (N=8) were aged 22 to 65 years (Mean=28.5) and all identified as male. Most of them were students (6), one full-time employee, and one retired. One participant was left-handed, and all others were right-handed. All participants stated to spend at least 1 hour per day at a desk, in particular, 1 to 9 hours (Mean=4.71) at work and/or 2 to 7 hours (Mean=3.86) privately. We also asked participants to select objects that they had on their desks. Most of them had a mouse, keyboard, and monitor (7 each); many also had a lamp (6), headphones (5), a laptop/tablet (4), or decoration (4); few had speakers (3) and a plant (1) on their desk. Participants additionally mentioned a printer and books (2 each).

6.2.6 Limitations. Study participants were not exposed to their own desks but to our controlled setup. Hence, the setup was not individualized with personal objects. This might have limited participants' experience. However, it helped us to gather first insights as to whether participants would generally accept such a concept.

6.3 Results

We present results from the questionnaires, analyzing the secrets themselves, and qualitative insights from the semi-structured interviews. Due to the exploratory nature of our study, we focus on descriptive and qualitative insights.

6.3.1 Secrets. We now describe how participants chose their authentication secrets.

Length. Participants chose longer secrets for very secure as compared to semi-secure secrets for both secret types (cf. Table 5 for descriptors of secret lengths). *Act2Auth* secrets consisted of 3 to 39 object touches and covered a wider range of lengths than text passwords (5 to 30 characters).

Objects. Participants often included actual objects in their secrets rather than touchpoints on the pad itself (cf. Figure 6). The right speaker was chosen most often (15), followed by the laptop (12) and decoration (10). However, three participants exclusively used touchpoints on the pad, e.g. by swiping over the lower row of touchpoints (P7) or using touchpoints close to the dominant (left) hand in the corner of the pad (P8).

Considerations. For the *Act2Auth* secret, most participants focused on *memorability* (P2, P4-7). P2 explicitly stated to have used a narrative for usual desk activities for the very secure, and a private anecdote for the semi-secure *Act2Auth* secret to foster memorability. P7 and P8 chose objects in visual patterns to be able to memorize them. For the very secure *Act2Auth* secret, P1 avoided points that could be hit accidentally. P2 used geometrical shapes and easy-to-remember objects (e.g., P2 used the plant in both secrets). For the semi-secure *Act2Auth* secret, P5 and P7 focused on input speed.

Memorability. Participants mainly agreed that they can easily memorize both secret types (on a 5-point Likert, cf. Figure 7a). However, we found that text passwords were reported as easier to remember than *Act2Auth* secrets. We also calculated Levenshtein distances[13] between the defined and memorized secret (cf. Table 5). Results show that participants were mostly able to correctly remember their semi-secure secrets (no errors for text passwords, 0.57 errors for *Act2Auth* secrets). Performance was worse for the very secure secrets with 2.28 errors made in the *Act2Auth* secret condition and 1.88 errors for the text password.

6.3.2 Security & Potential Threats. Participants assessed their secrets as rather secure (cf. Figure 7b). They also considered their stronger secrets to be more secure for both, *Act2Auth* secrets and text passwords. Participants rather disagreed that their secrets could be guessed by acquaintances or strangers (cf. Figures 7c and 7d).

[13]The Levenshtein distance describes the number of differences between two strings. See https://devopedia.org/levenshtein-distance for more details, last accessed December 10, 2023.

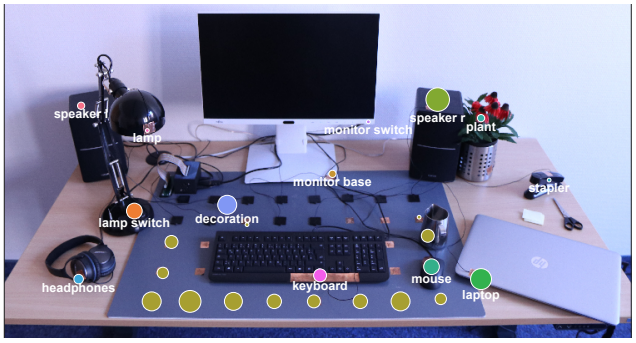


Figure 6: Distribution of selected objects in the lab study. Larger areas indicate that the respective object was selected by more participants. Non-labeled points correspond to capacitive touchpoints on the desk pad.

Participants found *Act2Auth* secrets hard to observe and memorize ad-hoc by a potential attacker (P1, P3, P6) as input might be subtle and not recognizable as secret (assuming the attacker does not know the mechanism). *Act2Auth* secrets might also be hard to guess as no "standard passwords" exist (yet) (P2). However, participants were concerned about the limited number of touchpoints resulting in a limited password space (P3 and P8). P2 and P8 mentioned that hints on typical inputs might exist and "sweet spots" in the password space might evolve (i.e., some objects might be chosen way more often than others). P8 explicitly expressed concerns about guessing by known people, as being left-handed influenced their choice of touchpoints.

To increase the security of their *Act2Auth* secrets, participants avoided choosing objects in an obvious pattern (P1 and P2), created longer (P3, P4, P8) or more complex input sequences (P7), or added additional inputs apart from their usual desk routine (P6). For text passwords, participants applied common strategies [53] such as adding special characters to increase security (P2, P5, P6) or replacing letters with numbers (P4, P7). Participants also aimed to prevent guessing by choosing complex passwords (P2, P5, P7).

To mitigate observation attacks, participants reported having tried to "hide" the input within their normal desk behavior (P2, P3, P6) or with their body (P7, P8). P5 and P8 reported they would make sure that no potential observer is present in the first place and/or send the person away. Overall, unobserved secret entry was perceived easier (Median=4, cf. Figure 8a) compared to the observed condition (Median=3, cf. Figure 8b).

Many participants found it hard to cover their input while using our prototype (P1, P5, P7, P8) as they, e.g. chose far away objects (P1). P8 even suggested a blanket to cover the setup. To mitigate observation attacks for the text passwords, participants likewise covered their input (P2-4, P6-8), but also entered their secrets as fast as possible to make observations more difficult (P1, P5).

6.3.3 Comparison & Concerns. We were especially interested in how *Act2Auth* would perform compared to a conventional input mechanism such as text on a keyboard. Entering both types of secrets, text and *Act2Auth* secrets was mostly considered fast and easy (on 5-point Likert scales, cf. Figure 8).

Participants mentioned that *Act2Auth* was new, hence unusual to them (P1, P2, P7, P8), and that this limited their capacity to freely create "creative" secrets. Moreover, the theoretical password space of *Act2Auth* was considered smaller and input was harder to hide for participants compared to keyboard input. However, participants liked the idea and prototype in general (P1, P2, P5). They appreciated that spatial features and personal objects might enhance memorability, which might become more apparent when using *Act2Auth* at their individual desk.

7 DISCUSSION & FUTURE RESEARCH DIRECTIONS

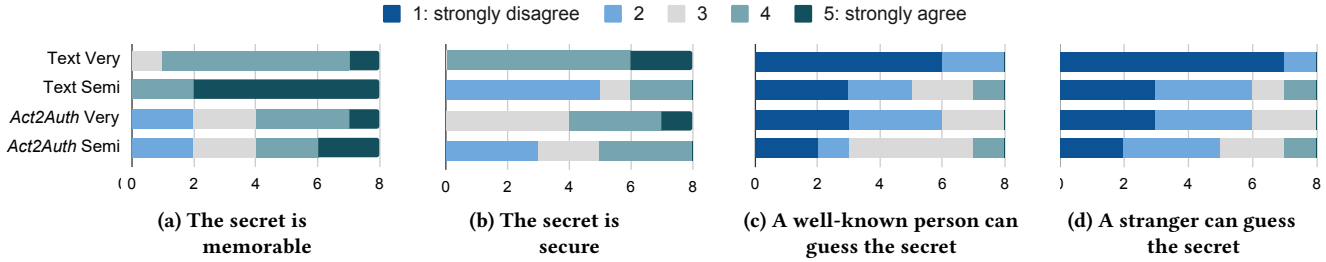
7.1 *Act2Auth* Secret Composition

Act2Auth allows for authentication based on tangible interactions with different types of physical objects (cf. Section 5). To evaluate how users would actually create such *Act2Auth* secrets and their underlying considerations, we explicitly asked participants in our studies to create them "from scratch". We found that they considered spatial relations and specific objects. They also leveraged the customizability of *Act2Auth* and focused on memorable secrets.

7.1.1 Leveraging Spatial Relations. With *Act2Auth*, we can leverage users' physical desk setup as a spatial context for authentication. Hence, contrary to most established knowledge-based authentication mechanisms, *Act2Auth* provides a meaningful spatial context to authentication and supports spatially distributed inputs. As such, users can compose secrets of near as well as far-away objects, which are easier or more complex to reach. They can also end their secret at an object that is near their next planned interaction, such as their mouse. Another option is to use spatial "patterns" within the desk setup (P7 and P8 in our lab study), similar to patterns on keyboards or PIN pads for conventional passwords. This can leverage users' motor memory and, thus, further increase the usability of the overall authentication procedure. Hence, our results indicate that *providing a meaningful spatial context for knowledge-based authentication can improve usability, as well as memorability.*

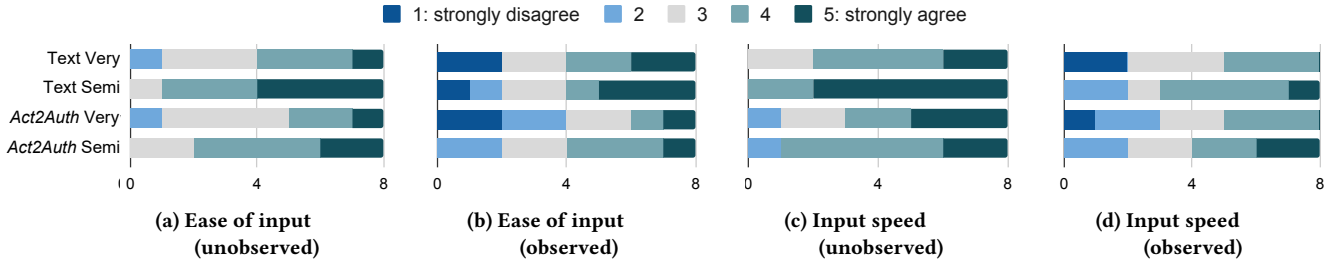
7.1.2 Object Characteristics. Participants in both, the online survey and lab study, involved objects of different types in their secrets. In particular, this not only included static objects on the desk (such as a speaker, decoration item, or plant pot) but also objects that potentially move. For instance, headphones, office supplies, or the mouse can be part of the *Act2Auth* secret. Note that the latter category of objects might move within the physical desk space, but also beyond as objects are taken to somewhere else (e.g., headphones). As such, the *password space can dynamically change* and, thus, hinder attackers from guessing the secret.

7.1.3 Customizability. *Act2Auth* secrets are customizable in different ways. *Act2Auth* can be used at people's desk setups that include their personal objects. Moreover, users can choose which objects on the desk to use for authentication. Users can also decide to which extent they want to integrate *Act2Auth* secrets into existing routines, or whether they would rather create new routines for authentication. The participants of our lab study took advantage of the customizability supported by *Act2Auth* by selecting a large



(a) The secret is memorable **(b) The secret is secure** **(c) A well-known person can guess the secret** **(d) A stranger can guess the secret**

Figure 7: Perceived secret memorability and security on 5-point Likert scales.



(a) Ease of input (unobserved) **(b) Ease of input (observed)** **(c) Input speed (unobserved)** **(d) Input speed (observed)**

Figure 8: Usability assessment of secret input on 5-point Likert items.

variety of different objects for authentication. They also appreciated the possibility of integrating *Act2Auth* into their personal desk setups and considered integrating authentication into their usual desk routines. Therefore, we see the *high level of customizability supported by Act2Auth as important for the adoption of embedded tangible authentication.*

7.1.4 Memorability. A common problem with knowledge-based authentication (such as PINs, passwords) is that users need to *memorize* a secret, which becomes challenging with the number of logins rising (e.g., for various devices or accounts) [2, 21]. At the same time, particularly secure secrets are typically long and complex (e.g., no dictionary words, special characters), and thus even harder to remember. With *Act2Auth*, we hope to foster memorability by the use of individual objects for the authentication secret.

In our study, participants reported they found text passwords still easier to remember. However, we did not analyze the actual text they chose as passwords, but only metadata such as length. As such, we cannot make assumptions about, e.g., dictionary words being (part of) these passwords, which would obviously be easy to remember, but critical from a security perspective. Overall, participants considered secrets they chose to be more secure to also be harder to memorize, which is in line with conventional text passwords. It will be interesting to see if there exists *a break even, where the memorability of* Act2Auth *secrets outperforms the memorability of (too simple) text-based secrets.*

At the same time, participants indeed had different strategies to enhance memorability, e.g. creating stories or making use of metaphors. This might be further elaborated by using *Act2Auth* at personal desks with known objects. Using *Act2Auth* over time, *existing routines can be leveraged, and motor memory can help to remember the secret.*

7.2 Embedded Authentication with *Act2Auth*

As discussed in Section 5, authentication with *Act2Auth* can be embedded into users' routines and environments. Participants in both, the online survey and lab study, leveraged this possibility and suggested involving their usual desk routines, personal stories, or metaphors. They further appreciated the option to use their personal objects for an *Act2Auth* secret. This increases or even dynamically changes the password space per individual user. In comparison, users cannot customize, for example, the password space for traditional text passwords as they must consist of letters, numbers, and special characters.

Our participants particularly liked these features of *Act2Auth*: a) embedding authentication in a way that could be perceived less as a barrier and more as a natural part of our daily lives and b) the possibility to customize authentication secrets in a way that is unique for each user. Hence, we see a promising trend that motivates future research on embedded authentication specifically in desk setups, but also in other environments. For example, further research should be carried out to allow users to experience *Act2Auth* at their personal desks, *to allow for fully embedding authentication in personal routines.*

7.3 Applicability of *Act2Auth*

We consider *Act2Auth* particularly useful for the "main" authentication necessary at desks: unlocking the PC or laptop. This is often part of a longer routine that may include, e.g., approaching the desk, putting other items down, sitting down in the chair, and touching or moving items on the desk. This allows embedding *Act2Auth*-based authentication into this routine and entering the authentication secret even before the user specifically interacts with the PC.

Other scenarios include access to a certain functionality or software such as, e.g., an e-mail client. However, such authentication actions are usually much more frequent. As participants did not rate the usability of *Act2Auth* as explicitly better compared to text passwords, we expect similar annoyance or fatigue effects to arise when users are required to enter *Act2Auth* secrets too frequently. Also, a high number of varying *Act2Auth* secrets might still exceed users' memory, albeit using metaphors or similar techniques. One established solution to reducing these effects is using password managers. We believe that password managers also represent a suitable option in the context of *Act2Auth* (i.e., by implementing password managers that can emulate *Act2Auth* secrets). Future research could identify more *application scenarios that are especially suitable for Act2Auth-based authentication.*

7.4 Protecting Tangible Multi-Object Secrets

An authentication secret should be kept with the legitimate user, and input not be overseen by others. Accordingly, users often show protective behavior with regard to knowledge-based authentication (e.g., covering a pin entry with their hand). Since *Act2Auth* leverages tangible interactions with multiple physical objects for authentication, we observed protective behavior specific to this input modality. Participants in our lab study were exposed to an *observation* scenario, i.e., somebody observing their input. To *mitigate observation* of the *Act2Auth* secret, common strategies of participants were to hide input with their body; to add additional interactions not being part of the secret; or to enter their secret subtly. Moreover, participants in both the online survey and the lab study were worried that strangers and well-known persons could *guess* their secret. To counteract this, participants involved "unusual" (i.e., hard to guess) or "far away" objects in their secrets, chose unusual touchpoints within objects, added duplicates, or increased length.

Our insights on these behaviors can assist future researchers in developing multi-object tangible authentication mechanisms that by design eliminate the need for specific behaviors or support users in performing them. For example, *we envision such future mechanisms to allow for subtle input (e.g., invisible touchpoints or sensors) and additional input that is recognized by the system as not being part of the authentication secret.*

7.5 Future Implementations of *Act2Auth*

In this work, we focused on tangible interactions at desks, to leverage these for authentication. However, we believe that this concept can, in the future, be used in other scenarios as well. Think about, e.g., tangible interactions in the home context such as at the door [10, 19, 39] or in the kitchen [20]. Outside the home, we further envision other (semi-)private environments, which require authentication, such as non-desk-based workplaces or cars to be suitable for mechanisms similar to *Act2Auth*.

Moreover, we envision future implementations of *Act2Auth* to allow for more fine-grained touch sensing, reduce the number of wires used for sensing, as well as leverage multiple sensor types for e.g., inertial measurements [19, 20, 65]. This would allow for measuring and distinguishing a larger variety of tangible interactions, such as moving objects, shaking, or tilting them [46].

Furthermore, analyzing users' behavior while interacting with objects (e.g., applied pressure or time between two objects) could serve as additional input metrics. Combining knowledge with behavioral features has been previously proposed for smartphone unlock patterns (e.g., [9]).

8 CONCLUSION

We propose *Act2Auth*, a novel concept for embedding authentication in tangible interactions with daily life objects at desks. We informed *Act2Auth* through findings regarding people's typical desk setups, an online survey on how people would create touch-based authentication secrets ($N = 65$), and a technical exploration of touch sensing in this environment. Next, we evaluated our concept in a lab study ($N = 8$) using a real-world prototype. We found that participants overall liked aspects of *Act2Auth* and were able to choose authentication secrets they considered usable as well as secure. Our work serves as a fundament for future research on embedding authentication into users' routines and environments.

ACKNOWLEDGMENTS

We would like to thank our study participants for their time and valuable input. This project has been funded by the European Union – NextGeneration EU, the dtec.bw – Center for Digitization and Technology Research of the Bundeswehr (projects MuQuaNet and Voice of Wisdom) and the German Research Foundation (DFG) under project no. 425869382.

REFERENCES

[1] Ghazanfer Abbas, Shah Rukh Humayoun, Ragaad AlTarawneh, and Achim Ebert. 2018. Simple Shape-Based Touch Behavioral Biometrics Authentication for Smart Mobiles. In *Proceedings of the 2018 International Conference on Advanced Visual Interfaces* (Castiglione della Pescaia, Grosseto, Italy) *(AVI '18)*. Association for Computing Machinery, New York, NY, USA, Article 50, 3 pages. https://doi.org/10.1145/3206505.3206571

[2] Anne Adams and Martina Angela Sasse. 1999. Users Are Not the Enemy. *Commun. ACM* 42, 12 (dec 1999), 40–46. https://doi.org/10.1145/322796.322806

[3] 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. https://doi.org/10.1109/TIM.2008.919905

[4] Szilvia Balogh, Tobias Daniel, Sarah Delgado Rodriguez, Ismael Prieto Romero, and Florian Alt. 2022. Rubik's Cube Auth - A Tangible Authentication Mechanism Using A Standard Rubik's Cube. In *Mensch und Computer 2022 - Workshopband*. Gesellschaft für Informatik e.V., Bonn.

[5] Francesco Bergadano, Daniele Gunetti, and Claudia Picardi. 2002. User Authentication through Keystroke Dynamics. *ACM Trans. Inf. Syst. Secur.* 5, 4 (nov 2002), 367–397. https://doi.org/10.1145/581271.581272

[6] Rasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. 2015. Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption. (2015).

[7] Virginia Braun and Victoria Clarke. 2012. Thematic analysis. (2012).

[8] Heather Crawford and Karen Renaud. 2014. Understanding user perceptions of transparent authentication on a mobile device. *Journal of Trust Management* 1 (2014), 1–28.

[9] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. 2012. Touch Me Once and i Know It's You! Implicit Authentication Based on Touch Screen Patterns. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Austin, Texas, USA) *(CHI '12)*. Association for Computing Machinery, New York, NY, USA, 987–996. https://doi.org/10.1145/2207676.2208544

[10] Sarah Delgado Rodriguez, Lukas Mecke, and Florian Alt. 2022. SenseHandle: Investigating Human-Door Interaction Behaviour for Authentication in the Physical World. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*. 7–9.

[11] Sarah Delgado Rodriguez, Sarah Prange, Lukas 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, Article 325, 6 pages. https://doi.org/10.1145/3411763.3451825

[12] Paul H. Dietz and Benjamin D. Eidelson. 2009. SurfaceWare: Dynamic Tagging for Microsoft Surface. In *Proceedings of the 3rd International Conference on Tangible and Embedded Interaction* (Cambridge, United Kingdom) *(TEI '09)*. Association for Computing Machinery, New York, NY, USA, 249–254. https://doi.org/10.1145/1517664.1517717

[13] Jayesh Doolani, Matthew Wright, Rajesh Setty, and S M Taiabul Haque. 2021. LociMotion: Towards Learning a Strong Authentication Secret in a Single Session. 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 689, 13 pages. https://doi.org/10.1145/3411764.3445105

[14] Rainhard Dieter Findling, Muhammad Muaaz, Daniel Hintze, and René Mayrhofer. 2017. ShakeUnlock: Securely Transfer Authentication States Between Mobile Devices. *IEEE Transactions on Mobile Computing* 16, 4 (2017), 1163–1175. https://doi.org/10.1109/TMC.2016.2582489

[15] Kyosuke Futami, Akari Fukao, and Kazuya Murao. 2019. A Method to Recognize Entering and Leaving Person Based on Door Opening and Closing Movement Using Angular Velocity Sensor. In *Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers* (London, United Kingdom) *(UbiComp/ISWC '19 Adjunct)*. Association for Computing Machinery, New York, NY, USA, 57–60. https://doi.org/10.1145/3341162.3343798

[16] Ceenu George, Mohamed Khamis, Daniel Buschek, and Heinrich Hussmann. 2019. Investigating the Third Dimension for Authentication in Immersive Virtual Reality and in the Real World. In *2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*. 277–285. https://doi.org/10.1109/VR.2019.8797862

[17] Tobias Grosse-Puppendahl, Yannick Berghoefer, Andreas Braun, Raphael Wimmer, and Arjan Kuijper. 2013. OpenCapSense: A rapid prototyping toolkit for pervasive interaction using capacitive sensing. In *2013 IEEE International Conference on Pervasive Computing and Communications (PerCom)* (San Diego, CA, USA) *(PerCom '13)*. IEEE, 152–159.

[18] Tobias Grosse-Puppendahl, Sebastian Herber, Raphael Wimmer, Frank Englert, Sebastian Beck, Julian von Wilmsdorff, Reiner Wichert, and Arjan Kuijper. 2014. Capacitive Near-Field Communication for Ubiquitous Interaction and Perception. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Seattle, Washington) *(UbiComp '14)*. Association for Computing Machinery, New York, NY, USA, 231–242. https://doi.org/10.1145/2632048.2632053

[19] Sandeep Gupta, Attaullah Buriro, and Bruno Crispo. 2019. SmartHandle: A Novel Behavioral Biometric-Based Authentication Scheme for Smart Lock Systems. In *Proceedings of the 2019 3rd International Conference on Biometric Engineering and Applications* (Stockholm, Sweden) *(ICBEA 2019)*. Association for Computing Machinery, New York, NY, USA, 15–22. https://doi.org/10.1145/3345336.3345344

[20] Jun Han, Shijia Pan, Manal Kumar Sinha, Hae Young Noh, Pei Zhang, and Patrick Tague. 2017. Sensetribute: Smart Home Occupant Identification via Fusion across on-Object Sensing Devices. In *Proceedings of the 4th ACM International Conference on Systems for Energy-Efficient Built Environments* (Delft, Netherlands) *(BuildSys '17)*. Association for Computing Machinery, New York, NY, USA, Article 2, 10 pages. https://doi.org/10.1145/3137133.3137152

[21] Marian Harbach, Alexander De Luca, and Serge Egelman. 2016. The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 4806–4817. https://doi.org/10.1145/2858036.2858267

[22] Chiung Ching Ho, C. Eswaran, Kok-Why Ng, and June-Yee Leow. 2012. An Unobtrusive Android Person Verification Using Accelerometer Based Gait. In *Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia* (Bali, Indonesia) *(MoMM '12)*. Association for Computing Machinery, New York, NY, USA, 271–274. https://doi.org/10.1145/2428955.2429007

[23] Christian Holz and Marius Knaust. 2015. Biometric Touch Sensing: Seamlessly Augmenting Each Touch with Continuous Authentication. In *Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology* (Charlotte, NC, USA) *(UIST '15)*. Association for Computing Machinery, New York, NY, USA, 303–312. https://doi.org/10.1145/2807442.2807458

[24] Sergi Jordà, Günter Geiger, Marcos Alonso, and Martin Kaltenbrunner. 2007. The ReacTable: Exploring the Synergy between Live Music Performance and Tabletop Tangible Interfaces. In *Proceedings of the 1st International Conference on Tangible and Embedded Interaction* (Baton Rouge, Louisiana) *(TEI '07)*. Association for Computing Machinery, New York, NY, USA, 139–146. https://doi.org/10.1145/1226969.1226998

[25] Zach Jorgensen and Ting Yu. 2011. On Mouse Dynamics as a Behavioral Biometric for Authentication. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (Hong Kong, China) *(ASIACCS '11)*. Association for Computing Machinery, New York, NY, USA, 476–482. https://doi.org/10.1145/1966913.1966983

[26] Zach Jorgensen and Ting Yu. 2011. On Mouse Dynamics as a Behavioral Biometric for Authentication. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (Hong Kong, China) *(ASIACCS '11)*. Association for Computing Machinery, New York, NY, USA, 476–482. https://doi.org/10.1145/1966913.1966983

[27] Hassan Khan, Urs Hengartner, and Daniel Vogel. 2015. Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 225–239. https://www.usenix.org/conference/soups2015/proceedings/presentation/khan

[28] Tomi Kinnunen, Filip Sedlak, and Roman Bednarik. 2010. Towards Task-Independent Person Authentication Using Eye Movement Signals. In *Proceedings of the 2010 Symposium on Eye-Tracking Research & Applications* (Austin, Texas) *(ETRA '10)*. Association for Computing Machinery, New York, NY, USA, 187–190. https://doi.org/10.1145/1743666.1743712

[29] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, and Pranjal Rathod. 2013. Secure authentication with 3D password. *International Journal of Engineering Science and Innovative Technology (IJESIT)* 2, 2 (2013), 99–105.

[30] Andraž Krašovec, Daniel Pellarini, Dimitrios Geneiatakis, Gianmarco Baldini, and Veljko Pejović. 2020. Not Quite Yourself Today: Behaviour-Based Continuous Authentication in IoT Environments. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 4, 4, Article 136 (dec 2020), 29 pages. https://doi.org/10.1145/3432206

[31] Sowndarya Krishnamoorthy, Luis Rueda, Sherif Saad, and Haytham Elmiligi. 2018. Identification of User Behavioral Biometrics for Authentication Using Keystroke Dynamics and Machine Learning. In *Proceedings of the 2018 2nd International Conference on Biometric Engineering and Applications* (Amsterdam, Netherlands) *(ICBEA '18)*. Association for Computing Machinery, New York, NY, USA, 50–57. https://doi.org/10.1145/3230820.3230829

[32] Juho Leinonen, Krista Longi, Arto Klami, Alireza Ahadi, and Arto Vihavainen. 2016. Typing Patterns and Authentication in Practical Programming Exams. In *Proceedings of the 2016 ACM Conference on Innovation and Technology in Computer Science Education* (Arequipa, Peru) *(ITiCSE '16)*. Association for Computing Machinery, New York, NY, USA, 160–165. https://doi.org/10.1145/2899415.2899472

[33] J. Leitner, M. Haller, K. Yun, W. Woo, M. Sugimoto, M. Inami, A. D. Cheok, and H. D. Been-Lirn. 2010. Physical Interfaces for Tabletop Games. *Comput. Entertain.* 7, 4, Article 61 (jan 2010), 21 pages. https://doi.org/10.1145/1658866.1658880

[34] Xiaopeng Li, Fengyao Yan, Fei Zuo, Qiang Zeng, and Lannan Luo. 2019. Touch Well Before Use: Intuitive and Secure Authentication for IoT Devices. In *The 25th Annual International Conference on Mobile Computing and Networking* (Los Cabos, Mexico) *(MobiCom '19)*. Association for Computing Machinery, New York, NY, USA, Article 33, 17 pages. https://doi.org/10.1145/3300061.3345434

[35] Jonathan Liebers, Uwe Gruenefeld, Daniel Buschek, Florian Alt, and Stefan Schneegass. 2023. Introduction to Authentication Using Behavioral Biometrics. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI EA '23)*. Association for Computing Machinery, New York, NY, USA, Article 547, 4 pages. https://doi.org/10.1145/3544549.3574190

[36] Jonathan Liebers, Patrick Horn, Christian Burschik, Uwe Gruenefeld, and Stefan Schneegass. 2021. Using Gaze Behavior and Head Orientation for Implicit Identification in Virtual Reality. In *Proceedings of the 27th ACM Symposium on Virtual Reality Software and Technology* (Osaka, Japan) *(VRST '21)*. Association for Computing Machinery, New York, NY, USA, Article 22, 9 pages. https://doi.org/10.1145/3489849.3489880

[37] Sana Maqsood, Sonia Chiasson, and Audrey Girouard. 2016. Bend Passwords: using gestures to authenticate on flexible devices. *Personal and Ubiquitous Computing* 20 (2016), 573–600.

[38] 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

[39] Lukas Mecke, Ken Pfeuffer, Sarah Prange, and Florian Alt. 2018. Open Sesame! User Perception of Physical, Biometric, and Behavioural Authentication Concepts to Open Doors. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia* (Cairo, Egypt) *(MUM '18)*. Association for Computing Machinery, New York, NY, USA, 153–159. https://doi.org/10.1145/3282894.3282923

[40] 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

[41] Muhammad Muaaz and René Mayrhofer. 2013. An Analysis of Different Approaches to Gait Recognition Using Cell Phone Based Accelerometers. In *Proceedings of International Conference on Advances in Mobile Computing & Multimedia* (Vienna, Austria) *(MoMM '13)*. Association for Computing Machinery, New York, NY, USA, 293–300. https://doi.org/10.1145/2536853.2536895

[42] Muhammad Muaaz and René Mayrhofer. 2014. Orientation Independent Cell Phone Based Gait Authentication. In *Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia* (Kaohsiung, Taiwan) *(MoMM '14)*. Association for Computing Machinery, New York, NY, USA, 161–164. https://doi.org/10.1145/2684103.2684152

[43] L. O'Gorman. 2003. Comparing passwords, tokens, and biometrics for user authentication. *Proc. IEEE* 91, 12 (Dec 2003), 2021–2040. https://doi.org/10.1109/

JPROC.2003.819611

[44] Makoto Ono, Buntarou Shizuki, and Jiro Tanaka. 2013. Touch & Activate: Adding Interactivity to Existing Objects Using Active Acoustic Sensing. In *Proceedings of the 26th Annual ACM Symposium on User Interface Software and Technology* (St. Andrews, Scotland, United Kingdom) *(UIST '13)*. Association for Computing Machinery, New York, NY, USA, 31–40. https://doi.org/10.1145/2501988.2501989

[45] Maja Pusara and Carla E. Brodley. 2004. User Re-Authentication via Mouse Movements. In *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security* (Washington DC, USA) *(VizSEC/DMSEC '04)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/1029208.1029210

[46] Sarah Delgado Rodriguez, Oliver Hein, Ismael Prieto Romero, Lukas Mecke, Felix Dietz, Sarah Prange, and Florian Alt. 2023. Shake-It-All: A Toolkit for Sensing Tangible Interactions on Everyday Objects. (2023).

[47] Valkyrie Savage, Xiaohan Zhang, and Björn Hartmann. 2012. Midas: Fabricating Custom Capacitive Touch Sensors to Prototype Interactive Objects. In *Proceedings of the 25th Annual ACM Symposium on User Interface Software and Technology* (Cambridge, Massachusetts, USA) *(UIST '12)*. Association for Computing Machinery, New York, NY, USA, 579–588. https://doi.org/10.1145/2380116.2380189

[48] Martin Schmitz, Mohammadreza Khalilbeigi, Matthias Balwierz, Roman Lissermann, Max Mühlhäuser, and Jürgen Steimle. 2015. Capricate: A Fabrication Pipeline to Design and 3D Print Capacitive Touch Sensors for Interactive Objects. In *Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology* (Charlotte, NC, USA) *(UIST '15)*. Association for Computing Machinery, New York, NY, USA, 253–258. https://doi.org/10.1145/2807442.2807503

[49] Martin Schmitz, Florian Müller, Max Mühlhäuser, Jan Riemann, and Huy Viet Viet Le. 2021. Itsy-Bits: Fabrication and Recognition of 3D-Printed Tangibles with Small Footprints on Capacitive Touchscreens. 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 419, 12 pages. https://doi.org/10.1145/3411764.3445502

[50] D. Schweitzer, J. Boleng, C. Hughes, and L. Murphy. 2009. Visualizing keyboard pattern passwords. In *2009 6th International Workshop on Visualization for Cyber Security*. 69–73.

[51] Ivo Sluganovic, Marc Roeschlin, Kasper B. Rasmussen, and Ivan Martinovic. 2016. Using Reflexive Eye Movements for Fast Challenge-Response Authentication. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (Vienna, Austria) *(CCS '16)*. Association for Computing Machinery, New York, NY, USA, 1056–1067. https://doi.org/10.1145/2976749.2978311

[52] Anil Somayaji, David Mould, and Carson Brown. 2013. Towards Narrative Authentication: Or, against Boring Authentication. In *Proceedings of the 2013 New Security Paradigms Workshop* (Banff, Alberta, Canada) *(NSPW '13)*. Association for Computing Machinery, New York, NY, USA, 57–64. https://doi.org/10.1145/2535813.2535820

[53] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2015. " I Added'!'at the End to Make It Secure": Observing Password Creation in the Lab. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*. 123–140.

[54] Nicolas Villar, Daniel Cletheroe, Greg Saul, Christian Holz, Tim Regan, Oscar Salandin, Misha Sra, Hui-Shyong Yeo, William Field, and Haiyan Zhang. 2018. Project Zanzibar: A Portable and Flexible Tangible Interaction Platform. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, Article 515, 13 pages. https://doi.org/10.1145/3173574.3174089

[55] Simon Voelker, Christian Cherek, Jan Thar, Thorsten Karrer, Christian Thoresen, Kjell Ivar Øvergård, and Jan Borchers. 2015. PERCs: Persistently Trackable Tangibles on Capacitive Multi-Touch Displays. In *Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology* (Charlotte, NC, USA) *(UIST '15)*. Association for Computing Machinery, New York, NY, USA, 351–356. https://doi.org/10.1145/2807442.2807466

[56] Simon Voelker, Kosuke Nakajima, Christian Thoresen, Yuichi Itoh, Kjell Ivar Øvergård, and Jan Borchers. 2013. PUCs: Detecting Transparent, Passive Untouched Capacitive Widgets on Unmodified Multi-Touch Displays. In *Proceedings of the 2013 ACM International Conference on Interactive Tabletops and Surfaces* (St. Andrews, Scotland, United Kingdom) *(ITS '13)*. Association for Computing Machinery, New York, NY, USA, 101–104. https://doi.org/10.1145/2512349.2512791

[57] Dirk Weirich and Martina Angela Sasse. 2001. Pretty Good Persuasion: A First Step towards Effective Password Security in the Real World. In *Proceedings of the 2001 Workshop on New Security Paradigms* (Cloudcroft, New Mexico) *(NSPW '01)*. Association for Computing Machinery, New York, NY, USA, 137–143. https://doi.org/10.1145/508171.508195

[58] Mark Weiser and John Seely Brown. 1996. Designing calm technology. *PowerGrid Journal* 1, 1 (1996), 75–85.

[59] Roman Weiss and Alexander De Luca. 2008. PassShapes: Utilizing Stroke Based Authentication to Increase Password Memorability. In *Proceedings of the 5th Nordic Conference on Human-Computer Interaction: Building Bridges* (Lund, Sweden) *(NordiCHI '08)*. Association for Computing Machinery, New York, NY, USA, 383–392. https://doi.org/10.1145/1463160.1463202

[60] Pierre Wellner. 1991. The DigitalDesk Calculator: Tangible Manipulation on a Desk Top Display. In *Proceedings of the 4th Annual ACM Symposium on User Interface Software and Technology* (Hilton Head, South Carolina, USA) *(UIST '91)*. Association for Computing Machinery, New York, NY, USA, 27–33. https://doi.org/10.1145/120782.120785

[61] Pierre Wellner, Wendy Mackay, and Rich Gold. 1993. Back to the Real World. *Commun. ACM* 36, 7 (jul 1993), 24–26. https://doi.org/10.1145/159544.159555

[62] EJ Williams. 1949. Experimental designs balanced for the estimation of residual effects of treatments. *Australian Journal of Chemistry* 2, 2 (1949), 149–168.

[63] Raphael Wimmer, Matthias Kranz, Sebastian Boring, and Albrecht Schmidt. 2007. A Capacitive Sensing Toolkit for Pervasive Activity Detection and Recognition. In *Fifth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom'07)*. 171–180. https://doi.org/10.1109/PERCOM.2007.1

[64] Simon S. Woo, Ron Artstein, Elsi Kaiser, Xiao Le, and Jelena Mirkovic. 2019. Using Episodic Memory for User Authentication. *ACM Trans. Priv. Secur.* 22, 2, Article 11 (April 2019), 34 pages. https://doi.org/10.1145/3308992

[65] Chuxiong Wu, Xiaopeng Li, Fei Zuo, Lannan Luo, Xiaojiang Du, Jia Di, and Qiang Zeng. 2022. Use It-No Need to Shake It! Accurate Implicit Authentication for Everyday Objects with Smart Sensing. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 6, 3, Article 146 (sep 2022), 25 pages. https://doi.org/10.1145/3550322

[66] J. Yan, A. Blackwell, R. Anderson, and A. Grant. 2004. Password memorability and security: empirical results. *IEEE Security Privacy* 2, 5 (2004), 25–31.

[67] Zhenyu Yan, Qun Song, Rui Tan, Yang Li, and Adams Wai Kin Kong. 2019. Towards Touch-to-Access Device Authentication Using Induced Body Electric Potentials. In *The 25th Annual International Conference on Mobile Computing and Networking* (Los Cabos, Mexico) *(MobiCom '19)*. Association for Computing Machinery, New York, NY, USA, Article 23, 16 pages. https://doi.org/10.1145/3300061.3300118

[68] Marina Zamsheva, Ingo Deutschmann, David Julitz, and Andreas Bienert. 2020. Person Authentication with BehavioSense Using Keystroke Biometrics. In *Proceedings of the 2020 International Conference on Pattern Recognition and Intelligent Systems* (Athens, Greece) *(PRIS 2020)*. Association for Computing Machinery, New York, NY, USA, Article 23, 6 pages. https://doi.org/10.1145/3415048.3416118

[69] Yongtuo Zhang, Wen Hu, Weitao Xu, Chun Tung Chou, and Jiankun Hu. 2018. Continuous Authentication Using Eye Movement Response of Implicit Visual Stimuli. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1, 4, Article 177 (jan 2018), 22 pages. https://doi.org/10.1145/3161410

A EXPLORING DESK SETUPS

Table 6: To find objects that are common on desks, we analyzed pictures ($N = 107$) from an online forum. For our study setups – both, online survey and lab study – we used objects that occurred in more than 20% of the pictures with two exceptions: we used a laptop only (i.e., not an additional desktop PC) and added an additional, movable object in the form of a coffee cup.

Device/Object	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

B EXPLORING *ACT2AUTH*: AN ONLINE SURVEY

B.1 Survey Structure & Questions

The online survey consisted of six parts.

(1) *Intro & Consent.* We first explained the research project and data collection process. Only after participants gave consent, they could continue with the survey.
(2) *Act2Auth Trial.* Next, we explained the concept in more detail. Participants could try defining secrets as long and as often as they wished to get familiar with both, concept and implementation.
(3) *Secret Creation & Strategy.* We then asked participants to create a total of three authentication secrets in randomized order – one they considered to be weak, one medium, and one strong. After they had defined each secret, we asked participants in detail about their choice, including their considerations and perception of usability and security:
   - Please describe the process of choosing your weak password as detailed as possible. What were your considerations with regards to security and usability (e.g., I preferred objects closer to my dominant hand; I did (not) consider where to exactly touch the object; ...)?
   - Please list the properties that make your chosen password secure. Think about password policies as known from textual passwords (e.g., minimum length, usage of special characters, etc).
   - Please list the properties that make your chosen password usable.
   - Why did you choose this password?
   - For which application would you use this password (e.g., online shopping, online banking, social media, ...)?
   - The following person can enter my password correctly. [5-point Likert scales]
     - Somebody who observed my input.
     - Somebody who knows me well and guesses the password.
     - A stranger who guesses the password.
   - Please rate the following statements. Please consider the real concept for this question (i.e., touching physical objects on your desk). [5-point Likert scales]
     - Entering the password was fast.
     - Entering the password was easy.
     - The entered password is secure.
     - I can easily remember the password.
(4) *Demographics.* Afterwards we asked participants to provide their demographics, dominant hand, hours spent at a desk (work and/or home) per day, objects on the (most used) desk, and objects they would consider for *Act2Auth*.
(5) *Final Questions.* Finally, we asked participants whether they would use the concept in the future (5-point Likert scale), and to compare *Act2Auth* against PINs, patterns, passwords, fingerprint, or face recognition (5-point Likert scale). We provided a free text field to capture further comments:
   - Please describe your strategy to remember the passwords. Did you use any memory aids to remember the passwords (e.g., writing it down, taking a picture with your smartphone, making a screenshot)? [open text field]
   - I would use this mechanism at my desk. Please consider the real concept for this question (i.e., touching physical objects on your desk). [5-point Likert scale, "I can't tell."]
   - Please consider the real concept for this question (i.e., touching physical objects on your desk). If given the option, I would use this mechanism rather than: PINs | Lock Patterns | Passwords | Fingerprint | Face Unlock | a TAN [5-point Likert scale, "I can't tell."]
   - Did you use an external mouse for completing this survey? [yes, no, other]
   - Further comments [open text field]

C USABILITY EXPLORATION: *ACT2AUTH* PROTOTYPE AT A DESK

C.1 Study Design

We chose the following descriptions for authentication secret strength level:

a) semi secure: a password for an application that has access to data that participants do not consider sensitive
b) very secure: a password for an application that has access to data that participants do consider highly sensitive

C.2 Procedure

(1) *Intro & Consent.* We introduced participants to our general concept. They signed a consent form and then had the opportunity to try out the prototype by setting and repeating a test password.
(2) *Secret Creation.* They then created two SECRET TYPES for each SECRET STRENGTH (semi secure, very secure), one textual and one using *Act2Auth* (henceforth called *Act2Auth* secret), in counterbalanced order (cf. Section 6.2.2). To create a secret,

participants had to enter it twice (i.e., similar to a usual set and approve process). After creating a secret, participants assessed the memorability and security of their created secret on 5-point Likert scales (cf. Appendix C.3) and we asked them about their secret and strategies.

(3) *Secret Input.* Participants then entered the secret twice (OBSERVED and UNOBSERVED). After every input, participants answered 5-point Likert scales on ease and speed of input (cf. Appendix C.4). After both inputs (i.e., observed and unobserved), we additionally asked them about their strategy to mitigate a potential observation attack.

(4) *Demographics & Final Questions.* After participants finished both SECRET STRENGTHS, we complemented the session with demographic questions and a semi-structured interview on the concept and potential use cases.

(5) *Short-Term Memorability.* Lastly, participants had to enter all their SECRETS again in order of creation to capture short-term memorability performance.

(6) *End & Reimbursement.* We gave participants the opportunity for questions and/or feedback and reimbursed them.

C.3 Secret

For every secret type (text password, *Act2Auth* secret):

- The entered password is secure. [5-point Likert scale]
- I can easily memorize the password. [5-point Likert scale]
- For which application would you use this password? [Multiple choice]
- The following person can enter my password correctly. [5-point Likert scales]
  - Somebody who knows me well and guesses the password.
  - A stranger who guesses the password.

After creation, we additionally asked:

- What did you choose as a password?
- Please describe the process of choosing your strong password as detailed as possible. What were your considerations with regard to security and usability (e.g., I preferred objects closer to my dominant hand; I did (not) consider where to exactly touch the object; ...)?

C.4 Input Questionnaire

For every secret type (text password, *Act2Auth* secret) and every input (observed, unobserved):

- Entering the password was fast. [5-point Likert scale]
- Entering the password was easy. [5-point Likert scale]

After both inputs, we additionally asked:

- How did you handle the fact that somebody might have observed your input?

C.5 Final Interview Questions

- How was your experience with our prototype?
- How did you generally like the usability of our concept?
- How did you generally like the security of our concept?
- Can you think of other use cases for our concept (i.e., apart from authentication/login)?