3D-Auth: Two-Factor Authentication with Personalized 3D-Printed Items

Karola Marky[1,2], **Martin Schmitz**[1], **Verena Zimmermann**[1], **Martin Herbers**[1], **Kai Kunze**[2], **and Max Mühlhäuser**[1]
[1]Technische Universität Darmstadt, Darmstadt, Germany, [2]Keio University, Yokohama, Japan
{marky, schmitz, herbers, max}@tk.tu-darmstadt.de, zimmermann@psychologie.tu-darmstadt.de, kai@kmd.keio.ac.jp

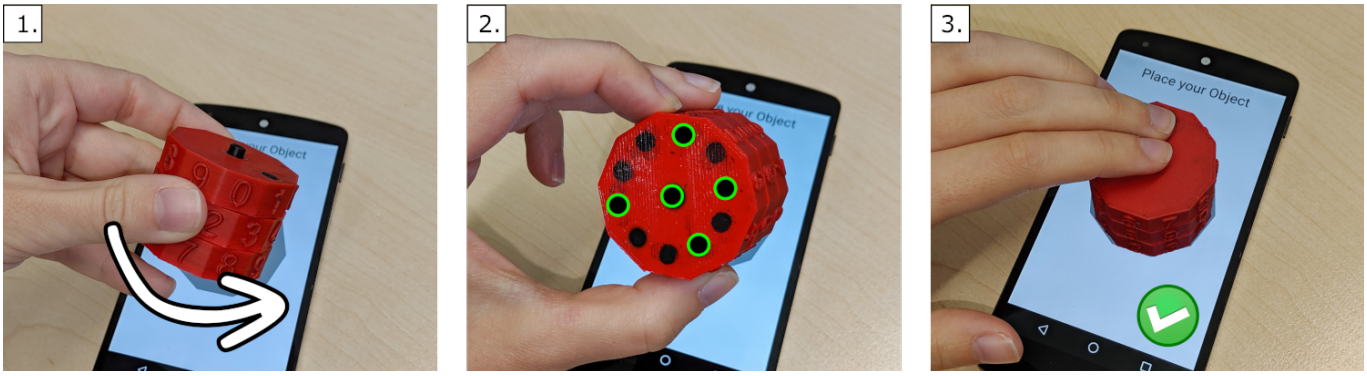


Figure 1. We present customizable 3D-printed items for authentication: the user interacts with the item in order to activate an authentication pattern on the object's bottom. The pattern is recognized by a touchscreen.

ABSTRACT
Two-factor authentication is a widely recommended security mechanism and already offered for different services. However, known methods and physical realizations exhibit considerable usability and customization issues. In this paper, we propose *3D-Auth*, a new concept of two-factor authentication. 3D-Auth is based on customizable 3D-printed items that combine two authentication factors in one object. The object bottom contains a uniform grid of conductive dots that are connected to a unique embedded structure inside the item. Based on the interaction with the item, different dots turn into touch-points and form an authentication pattern. This pattern can be recognized by a capacitive touchscreen. Based on an expert design study, we present an interaction space with six categories of possible authentication interactions. In a user study, we demonstrate the feasibility of 3D-Auth items and show that the items are easy to use and the interactions are easy to remember.

Author Keywords
Two-Factor Authentication; 3D Printing; Capacitive Sensing

CHI '20, April 25–30, 2020, Honolulu, HI, USA.

ACM ISBN 978-1-4503-6708-0/20/04 ...$15.00.
http://dx.doi.org/10.1145/3313831.3376189

CCS Concepts
•**Human-centered computing** → **Human computer interaction (HCI);** *Haptic devices;* User studies;

INTRODUCTION
With the proliferation of digital services, users have to authenticate themselves multiple times a day for a variety of tasks. For digital services that are security-critical, such as banking, two-factor authentication is a widely recommended authentication mechanism that enhances security [10, 6].

In two-factor authentication, two of the following authentication factors are combined: 1) knowledge (e.g., a password), 2) ownership (e.g., a credit card), and 3) inherence (e.g., a fingerprint) [15]. One factor often belongs to the category ownership and takes the form of a physical object, such as a token. Known methods of physical realizations of such objects exhibit considerable usability as well as customization issues [48, 8, 11, 2].

If users have the possibility to choose an authentication mechanism, their choice is primarily based on usability. Thus, usability issues lead to a low adoption rate [5, 32]. More specific, users perceive the duration of the current two-factor authentication procedures as too long [49] and they criticize the usage of non-personalized devices [48].

To tackle these usability and customization issues, we present *3D-Auth items*. 3D-Auth items are 3D-printed authentication items that combine the factors ownership and knowledge. The

3D-printed object encodes a secret using a conductive internal structure that can be uniquely customized and printed on demand. The object bottom contains a uniform grid that consists of several conductive dots. These dots are connected to the internal structure. Based on the interaction with the item, the internal structure changes and turns the dots on the bottom into touch-points. The touch-points form an authentication pattern that can be sensed by a capacitive touchscreen, e.g. on a standard smartphone. The possession of the item forms the first authentication factor and is not sufficient for a successful authentication. As the second factor, the user needs to correctly interact with the object in a pre-defined manner.

Based on the results of an expert design study, we present an interaction space with five categories of interactions. We realized one object per category as proof-of-concept and conducted a user study with 25 participants. We thereby add to the still scarce user evaluation research in that area [12]. The concept of the 3D-Auth items was welcomed by the participants as a possibility for two-factor authentication. The interactions were perceived as easy and efficient to perform and also easy to remember even after a retention of ten days.

3D-Auth items are not yet competing with other authentication mechanisms but serve as a stepping stone into a fully customizable two-factor authentication that could be printed at home on demand without the need of a provider for authentication items. Thus, our contribution presents a first step for addressing fundamental conceptual challenges.

Research Contributions

- We contribute an interaction space with five categories for interacting with 3D-printed items in the authentication context. The interaction space is based on two consecutive expert studies with 19 experts.
- We evaluated proof-of-concept items for our interaction space in a user study with 25 participants. The interactions are perceived as easy to perform and are also easy to remember.
- Furthermore, we provide a concept for securing 3D-Auth items for enabling a usable and customize two-factor authentication in one object.

BACKGROUND AND RELATED WORK

In this section, we present background and related work that our research builds upon. In particular, we detail *two-factor authentication*, *tangible authentication* as well as the *3D-printing of interactive objects*.

Two-Factor Authentication

Passwords are a knowledge-based authentication factor and the most commonly used authentication mechanism [44]. However, research has shown that users tend to follow a poor password hygiene by using passwords that are simple to guess and reusing passwords across multiple accounts [45, 47, 46]. This practice substantially weakens the security of passwords. Furthermore, service providers store the passwords in a database which might be attacked and leaked. Passwords are also susceptible to shoulder-surfing and phishing attacks. A possibility to mitigate the impact of these attacks are authentication mechanisms that combine different factors. The combination of two factors is called two-factor authentication. Multi-factor authentication combines more than two factors. A common example of two-factor authentication is the combination of a password or PIN (knowledge) and a token, such as a personal smart card (ownership).

Several schemes that enable two-factor authentication have been made available for end users in different contexts and on different platforms. Those schemes can rely on a physical token that generates one-time passwords, such as the DUO Security Token [42]. They can furthermore rely on text messages, e-mail notifications or apps on mobile devices. Previous work has explored a variety of these schemes. A usable configuration for enabling two-factor authentication that is technologically robust, however, has not been realized, yet [2].

The introduction of two-factor authentication has been investigated in several contexts. It has been shown that users prefer or choose devices that they already own over additional physical tokens [48]. Users also tend to choose devices for two-factor authentication based on their usability [49]. Ease-of-use, trustworthiness and the required cognitive effort were found as key aspects for defining the usability of two-factor authentication [13]. A study in the banking context shed light on the security-usability trade-off of two-factor authentication [16]: While two-factor authentication was perceived as more secure than single factor authentication, the perceived usability, ease-of-use and convenience were rated significantly lower. Authenticating with two-factor authentication also took longer compared to single factor authentication. However, if users have positive experiences with two-factor authentication, they might even use it for accounts that do not require it [9].

Tangible Authentication

Several approaches for tangible authentication have been proposed in the literature. Among those are wearable devices that have embedded cryptographic keys [7]. TangibleRubik provides tangible authentication by the manipulation of a Rubik's Cube [27]. Using TangibleRubik, a user's password consists of a series of moves with the tube, such as turning parts of it. These moves are captured by a webcam. A preliminary user study of TangibleRubik revealed that duration of password entry (34 and 52 seconds) were perceived as too long. Bend Passwords introduces tangible authentication with a flexible PVC sheet that has bend sensors [25]. A user study of Bend Passwords revealed that their perceived usability is lower than the usability of PINs. This indicates that the physical presentation of plays an integral role for usability.

3D Printing of Interactive Objects

Many works embed electrical components in objects to make them interactive. This can be achieved by mounting capacitive [33] or acoustic [29] sensors, or by embedding cameras [34] or accelerometers [17]. While these approaches require only a few components, they need additional assembly effort or only work with hollow objects that can be opened after printing.

Another stream of research is investigating how digital fabrication can be used to create customized interactive elements.

This includes the creation of input and output functions into 3D-printed objects by light pipes [3, 50], filling internal pipes with media after printing [35], or pipes that transmit sound [21]. Other approaches print interactive objects using conductive spray [19] or conductive plastic [4, 38, 20, 23, 37, 39, 36, 40]. 3D printing is also investigated for the fine-grained design of deformation behavior of non-interactive flexible objects [1, 30, 31, 41] or for the production of soft interactive objects [18].

EXPERT DESIGN STUDY

To generate interactions the users can perform for authentication, we conducted an expert design study with experts from different areas. Based on that, we refined the interaction space in an online study with 13 additional experts.

Methodology

We commenced with a focus group discussion. We opted for experts because they can reflect on the needs that users are typically unaware of. One expert can provide the expertise of multiple users [28].

We recruited six experts from our institution via mailing-lists. Their mean age was 31.8 years ($Min = 30$, $Max = 35$, $SD = 2$). All of them reported working in their field for over five years. We specifically chose to include two experts from the areas of usable security, human-computer interaction and IT-security to represent different perspectives. We opted for a focus group such that all experts can provide their expertise, and discuss and agree on distinct interaction concepts.

Study Setup

The experts were provided with 20 3D-printed objects in simple shapes, such as cubes. Each object was printed twice, one was printed in a non-flexible material (PLA) and one in a flexible material (Ninjaflex TPU). We also provided a smartphone and tablet-PC which we placed in the center of the table. Two cameras filmed the center of the table. The recording space was marked, such that the experts were aware of it.

Procedure

The procedure was as follows: First, we welcomed the experts and explained the goals of the discussion. We proceeded by explaining the consent form and the data protection policy which each expert signed. Then, each expert provided demographics.

We introduced the concept of the 3D-printed items and the setup and gave the experts time for familiarization. Then, we introduced the authentication scenario and the contexts that we aimed to consider in the study. In particular, we investigated the authentication contexts environment, device size, and task hierarchy from Gorlenko and Merrick [14]. We gradually introduced these contexts during the discussion. For each context, the experts provided interaction concepts with the 3D-printed items and demonstrated them with the smartphone and tablet. As a third device, we considered a smart meeting board that was not present in the room. The interaction concepts were written down on a piece of paper and pinned on a bulletin board next to the authentication context. We did not place any restrictions on the interaction concepts except that the 3D-printed item had to touch the device's touchscreen and the user's hand or finger had to touch the 3D-printed item, otherwise the item cannot be recognized by the touchscreen.

After discussing all of the presented authentication contexts, we reviewed and discussed the interaction concepts on the bulletin board with the experts. In this phase, the experts could add, refine or merge interaction concepts. We made sure that all interaction concepts were written down understandably. Then we stopped the recording, thanked the experts for their participation, and gave them the opportunity to ask questions and to provide additional feedback.

Focus Group and Online Study Results

The experts designed seventeen atomic interaction concepts. The notes from the bulletin board were transcribed into an electronic form and analyzed by an inductive categorization approach [26] by two of the paper's authors. The resulting categories represent groups of interaction concepts that we explain in the next section.

To investigate the interaction concepts from the focus group discussion with a larger group of experts, we conducted an online study with thirteen additional participants.

After reading and accepting the consent form as well as the data protection policy, each expert provided demographics. We provided an introductory text about the 3D-Auth items that was identical to the information that the focus group received. Then we provided the five categories from the focus group. In each category, we listed the interactions from the expert study and asked the experts to supplement them. If the expert chose to provide an interaction, we asked for a name and a description. Finally, the experts could provide additional feedback or comments in free-text format.

The study resulted in the new atomic interaction concept of gestures on the object's surface which fit into the category of touch. All other identified concepts were identical to those from the focus group.

INTERACTION SPACE

To authenticate with the 3D-Auth item, the user has to perform one or more interactions. As *interaction space*, we define the set of possible interactions. To design this interaction space, we conducted the expert design studies detailed above. In the remainder of the section, we present the categories of our interaction space as well as the atomic interaction concepts.

Touch

Touch represents the first category of interaction concepts in our interaction space. All concepts share that the users touch the object's surface in a specific way or spot. The following atomic interaction concepts belong to this category: 1) Touching the object in one spot. 2) Touching the object in multiple spots. 3) Pressing the object in one spot. 4) Pressing the object in multiple spots. 5) Performing a gesture on the object's surface (e.g, drawing a pattern). And 6) a combination thereof (e.g. a gesture + touch in in one spot)

Arrangement
The second category is based on the arrangement of one or more objects on the touchscreen. The arrangement could be a specific pattern or the positioning of the object in a certain location or orientation. The interaction concepts are: 1) Placing one object in a specific location and/or orientation, 2) moving an object on the touchscreen along a specific path, and 3) placing multiple objects in a static position on the touchscreen.

Assembly
For the assembly category, we consider objects that consist of different parts that can be assembled in a pre-defined way: 1) The first interaction concept is the stacking of objects (vertical assembly) and 2) the second one is the assembly of different parts horizontally. 3) Finally, horizontal and vertical assembly can be combined.

Configuration
For this category of interaction concepts, we consider objects which can be configured by the user. There are four concepts to change the configuration of an object: To do so, the first interaction concept is rotating movable parts of the object. The second concept is configuration by pressing object parts. Parts of the object can be slid to change its configuration. Finally, the electrical resistance of the object can be changed which is recognized by the touchscreen.

Augmentation
The configuration mentioned above targets the object itself while augmentation means that an object is augmented by something that is not part of the object itself. Here, we present the interaction concepts of 1) augmenting the object by filling it with water or 2) by filling the object with air.

3D-AUTH ITEMS

In this section, we explain the concept of the *3D-Auth items* that match five categories of our interaction space. We start with general *object principles* and the *overall password space*. Then, we proceed by describing *proof-of-concept prototypes* for each category.

Object Principles

A 3D-Auth item is printed with two materials. The first material is a conductive material (e.g., Proto-Pasta conductive PLA), which can be recognized by a capacitive touchscreen. The second material can be any insulating material (e.g., standard PLA). The conductive material is printed within the insulating material, such that it encodes a secret that is not visible from the outside but connected to it. This connection is made by conductive dots on the object's surface that need to be touched by the user. Only then, conductive dots at the bottom of the 3D-Auth item that touch the touchscreen are turned into touch-points dependent on the interaction. These touch-points form an authentication pattern.

Interactions that do not correspond to the user authentication interaction also activate touch-points. Thus, wrong patterns are possible and can be recognized by the touchscreen. This is important because otherwise an attacker that steals the 3D-Auth item might simply interact with it until they brute-force the correct pattern by trying every possible interaction.

Proof-of-Concept Prototypes

To evaluate the interactions within a user study, we developed five proof-of-concept prototypes, one for each category. All prototypes have similar dimensions, similar colors and are based on a simple shape to retain fair conditions in the user study. The prototypes were printed on a multi-material printer (Prusa MK3 with MMU2.0). Figure 2 on the following page depicts the prototypes and 3D models of them.

Touch Prototype: Touch Block
For the touch prototype, we used a square shape. The object has a uniform grid of conductive dots on the bottom. To recognize the touch interaction, we added a set of conductive dots to the object's top. Those dots are connected to those in the bottom by wires that are printed with the conductive material. By touching the dots at the top, the user turns conductive dots in the bottom into touch-points that can be sensed by the touchscreen.

The password space of the prototype touch item is 15 resulting from the requirement that the user could touch a selected combination of four dots with the exception that the number of touches points cannot be zero.

Arrangement Prototype: Slider
To built an arrangement prototype, we printed a 3D-object with a slider. The slider has ten possible positions which are labeled with the numbers from zero to nine. The adjuster of the slider is printed in a conductive material. Depending on its position, conductive dots in the object's bottom are turned into touch-points. We chose the position of the number five as target for the slider to perform the interaction. Since the slider can be arranged while being placed on the device's touchscreen, we added a button to the user interface which the user has to press once the arrangement is final.

The password space of the slider prototype consists of ten options equivalent to the ten numbers on the slider. However, for future uses the password space could be enlarged by combining several sliders, accepting positions in between numbers, or by having to move the slider to a sequence of positions.

Assembly Prototype: Building Blocks
The assembly prototype consists of four building blocks that can be connected via connectors. The connectors are printed with conductive material to enable a detection of the connection. The blocks can be connected to different shapes, such as an L-shape that we used for our user study. Based on that shape dots from in the object's bottom are turned into touch-points. But to activate them, the user has to touch at least one conductive dot or connector.

The number of possible shapes of the prototype with four blocks is nine. Each shape could be turned in 90° steps, thus the password space of the building blocks prototype was 36 minus the shapes that look the same turned by 180° such as a horizontal line, resulting in a final number of 26 options. This could be enhanced by increasing the number of blocks and therefore shapes, making the sequence of differently colored blocks matter, or allowing for turning the object in smaller than 90° steps.

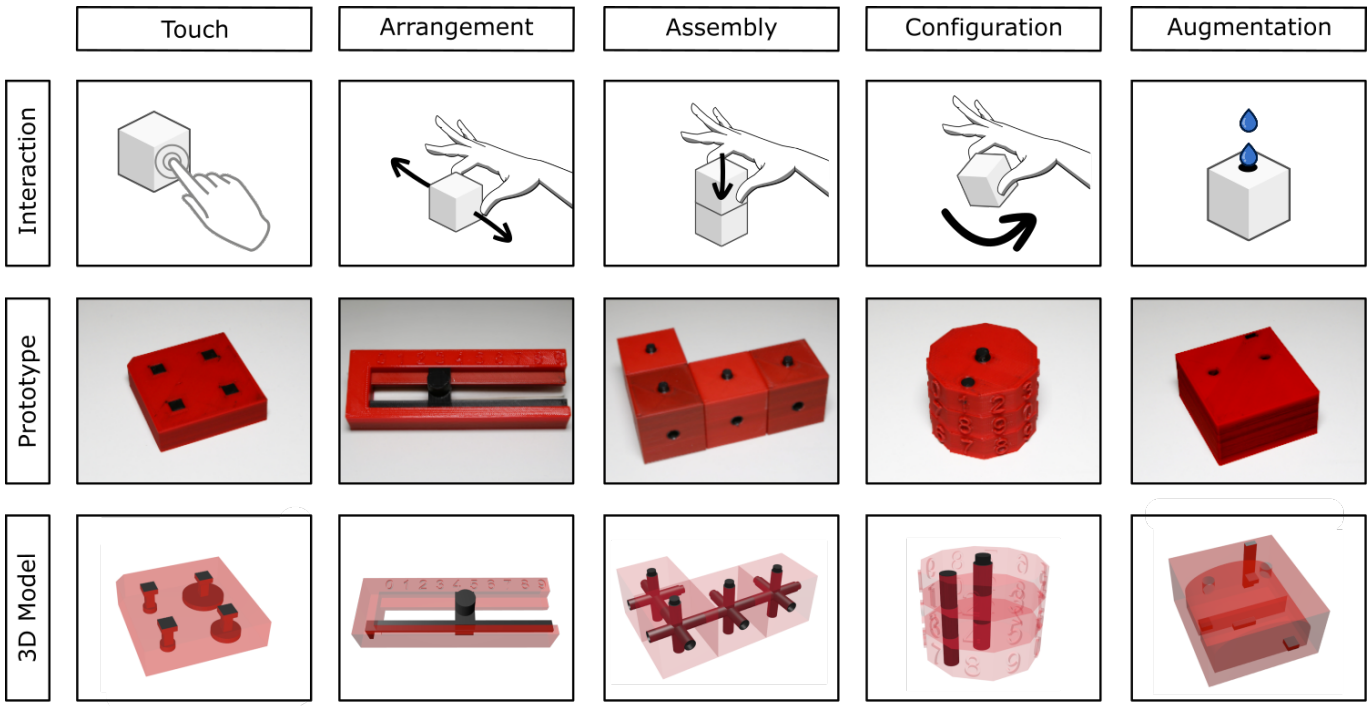


Figure 2. Proof-of-concept prototypes for the interaction categories. The prototypes do not constitute the only possibility to realize the interaction but serve as a basis for evaluation purposes.

Configuration Prototype: Combination Lock

To realize a configuration prototype, we printed a combination lock with three movable layers. The conductive dots in the bottom are turned into touch-points depending on the rotation of the individual layers. After configuring the combination lock by turning the layers, the user places it on the touch-screen and touches a conductive dot on the top to activate the authentication pattern. Each layer has ten possible positions.

The combination lock prototype has a password space of 10^3 which could further be increased for future implementations by increasing the amount of numbers on each layer or by increasing the number of layers.

Augmentation Prototype: Water Tank

For augmentation, we built a water tank. The object is a box with two internal chambers. One chamber has a capacity of 3.5*ml* of water. This amount can be filled into the object via a hole on the top, for instance with a syringe. The conductivity of the water connects conductive dots on the bottom. To activate the authentication pattern, the user has to touch a conductive dot on the object's top. If a user fills in more than the 3.5*ml* of water, the chamber overflows and the water fills the other chamber with activates further capacitive dots.

The prototype object differentiated between the correct amount of water, too much or too little water, leading to a password space of three possibilities. For future work, this space could be enlarged by refining the object's ability to differentiate between different water level steps or by dividing the object into several water tanks that require different amounts of water.

USER STUDY

To evaluate the proof-of-concept items detailed above, we conducted a user study with 25 participants. Our user study consisted of two parts: 1) a *lab study* and 2) a *retention study*.

Lab Study

We conducted a lab study to be able to control for environmental influences. We opted for a within-subject design to be able to compare the perceptions of the users regarding the different items. To avoid sequential effects, we counter-balanced the order of conditions by the Latin square.

Captured Data

Based on the ISO standard 9241-11, usability is compromises the dimensions of effectiveness, efficiency, and user satisfaction [43]. We implemented a smartphone app that was able to recognize the 3D-Auth items. With that app, we measured whether the participants successfully performed the interaction to assess the effectiveness. To evaluate efficiency, we measured the time for performing the authentication interaction. To capture the time, we recorded the interaction with a camera. The smartphone had a fixed position on the table and the camera was placed in a way that it did not record the participants' faces. For determining satisfaction, we used the user experience questionnaire [22] and open-ended questions, such as their opinion on the 3D-Auth items and the interactions they represent.

Study Procedure

An average study session took 15 minutes. The procedure of the lab study was as follows and aligns with the guidelines from the ethic's committee at our institution:

1. *Informed Consent.* The participants were explained the consent form and the data protection policy which they were asked to sign. The consent form, as well as the data protection policy, align with the General Data Protection Regulation (GDPR) in Europe.

2. *Familiarization.* We explained the concept of an 3D-Auth item to the participants. To do so, we provided this information as a text that each participant had to read. Then, we gave them 3D-printed objects of simple shapes, such that they could familiarize themselves with the haptics.

3. *Interaction and Questionnaires.* Each participant interacted with all 3D-Auth items in an order given by a Latin square. We provided each item together with an information sheet that explained the interaction. After reading the information sheet, the participant was asked to perform an authentication procedure on a smartphone. This procedure was repeated until the participant had interacted with all 3D-Auth items.

4. *Final Questionnaire.* After the interaction, the participants received a final questionnaire that included questions to compare the different 3D-Auth items. We furthermore asked whether the participants would use 3D-Auth items and if so, on which devices they would like to use them. We also provided the user experience questionnaire. Finally, the participants could ask questions about the study.

5. *Retention Study Explanation.* We invited the participants to the retention study (see below) and gave them the opportunity to freely interact with the 3D-Auth items. We furthermore answered questions regarding the correct execution of the interactions.

Retention Study

We investigated the memorability of the interactions after a duration of ten days. 40% of participants ($N = 10$) participating in the lab study returned for the retention study.

The procedure of the retention study was almost identical to the lab study. The only difference was that we did not provide the information sheets that described the interaction. Thus, the participants had to rely on their memory in terms of conducting the correct interactions. After the completion of all interactions, we again provided the user experience questionnaire and the same questions as in the lab study.

Participants

We recruited a sample of 25 participants by mailing-lists, poster advertisements, and word-of-mouth. The participants were on average 36.6 years old ($Min = 24$, $Max = 60$, $Median = 32$, $SD = 13$). Eight of them identified as female, one as other and one opted for "prefer not to say". We did not compensate the participants for taking part in our study.

USER STUDY RESULTS

In this section, we present the results from the lab, as well as the retention study.

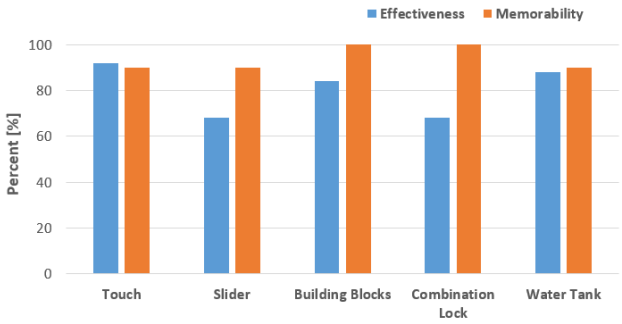


Figure 3. Effectiveness and memorability of the 3D-Auth items.

Effectiveness

As effectiveness, we considered the share of participants that correctly performed the authentication interaction. We furthermore used the video recordings to find out why an interaction was performed incorrectly. Overall, 80% of interactions were performed correctly. The distribution among the different items is depicted in Figure 3.

The touch item demonstrated the highest effectiveness rate with 92%. The reason for incorrect interactions was placing the item upside-down.

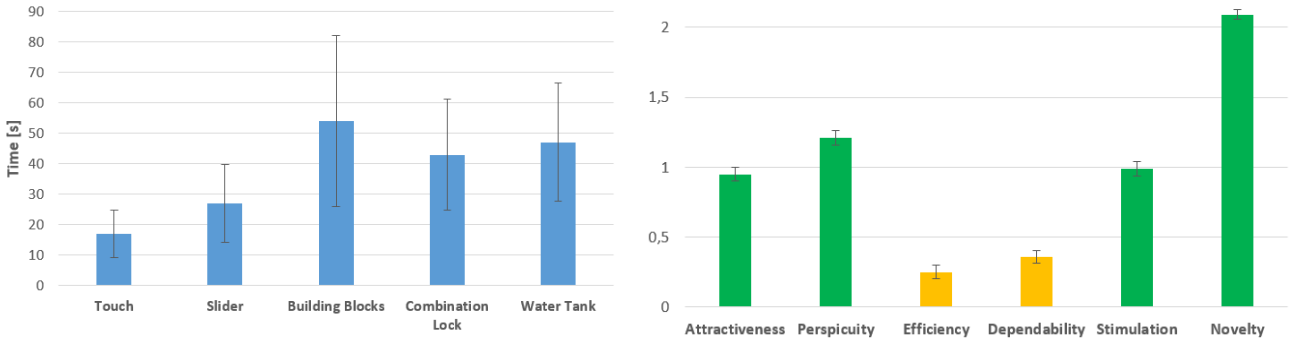
The items with the lowest effectiveness rate were the slider and the combination lock (68%). Although the combination lock was configured correctly, the participants either did not touch the conductive dots on the top or placed it in a wrong orientation. Also, the slider was arranged correctly, but the participants either did not press the button in the user interface or placed the slider in a wrong orientation even though the shape of the slider was depicted on the user interface.

84% of the participants correctly interacted with the building blocks. One participant just placed the blocks in the required shape without connecting them. The two other participants did not touch the conductive dots.

In terms of the water tank, 88% of the participants performed a correct interaction. Those who did not interact with it correctly, either put too much water in it or did not touch the conductive dot on top of the object.

Memorability

For memorability, we consider the share of participants that correctly performed the interaction after a retention of ten days. Each participant had a random participant number, such that we could connect the results from the lab and the retention study. Overall, 94% of the interactions were remembered correctly. The shares of the individual objects are given in Figure 3. The touch item was remembered by 90% of the participants. One participant remembered the interaction correctly, but placed it upside-down on the touchscreen. Similarly, one participant remembered the position of the slider correctly, but placed the slider in a wrong orientation on the touchscreen. Finally, one participant forgot the amount of water that had to be filled into the water tank.



(a) (b)

Figure 4. Results of our user study (a) depicts the execution time, and (b) depicts the user experience scales. Yellow bars depict a neutral evaluation and green ones depict a positive evaluation. The error bars in the UEQ scales indicate the standard error.

Efficiency

To perform one interaction the participants needed on average 37*s* ($Min = 16$, $Max = 54$, $SD = 15$). The durations to perform the interactions with the individual 3D-Auth prototypes are depicted in Figure 4a.

The touch block had the fastest interaction with an average of 17*s* ($Min = 10$, $Max = 40$, $SD = 7.7$). The second fastest was the slider with a mean duration of 27*s* ($Min = 7$, $Max = 60$, $SD = 12.9$). The participants needed on average 43*s* ($Min = 15$, $Max = 91$, $SD = 18.1$) to interact with the combination lock. While the participants did not exhibit any problems with configuring the combination, placing the item in the correct orientation required most of the time. Participants interacting with the water tank needed on average 47*s* ($Min = 12$, $Max = 90$, $SD = 19.4$). Hereby, filling in the water with the syringe took the majority of the time. Interacting with the building blocks took longest with an average of 54*s* ($Min = 25$, $Max = 135$, $SD = 28.1$). The reason for this is that the participants first examined the individual blocks to find out how to connect them.

User Experience

The user experience questionnaire assesses user experience in the six scales attractiveness, perspicuity, efficiency, dependability, stimulation and novelty [22]. Each scale ranges from -3 to 3. Values below -0.8 represent a *negative evaluation*, those between -0.8 and 0.8 represent a *neutral evaluation* and those above 0.8 means a *positive evaluation*. The scales efficiency and dependability received a neutral evaluation, all other scales received a positive one. The ratings are depicted in Figure 4b.

We opted not to rate individual prototypes, because this would have tripled the study duration. We furthermore aimed to start with measuring the user experience of the concept in general since the prototypes do not represent final 3D-Auth items.

User Perceptions and Preferences

In the final questionnaire, we asked the participants whether they would like to use the items in real life. The majority of participants (68%) intended to use the combination lock. When asked to explain their answers, the participants stated[1]:

- *"It's so easy to use."* (P1)
- *"Joy, easy to remember, practical."* (P8)
- *"Easy to use, no additional ingredients like water or anything are required and it's compact to store."* (P10)

The water tank was chosen by none of the participants. Reasons mentioned by the participants were:

- *"The water tank would be very cumbersome when you are on the road."* (P7)
- *"Too complicated for me."* (P11)

We asked which interaction or combination of interactions they would like to perform in the authentication context. 48% stated that they would like to use an interaction based on the configuration of an object like the combination lock. Sample comments given by the participants are:

- *"It's an easy solution that I already know from other domains."* (P6)
- *"Configuration is fun."* (P12)

36% of the participants would like to perform a touch interaction based on the simplicity and inconspicuousness of it:

- *"Touching is easy to do and needed with any item anyway."* (P11)
- *"I could do it in the dark or in my pocket."* (P25)

We proceeded by asking on which devices the participants would like to use 3D-Auth items. 36% would like to use the item for unlocking a smartphone because the smartphone is more likely to get stolen. The participants stated:

- *"In case my device gets stolen, it's more secure."* (P5)
- *"It would be an additional protection."* (P9)

44% would like to use on a larger touchscreen, such as a tablet-PC or laptop. As a reason they stated that the devices are mostly used in a static location:

[1] All answers were translated from German.

- *"I often have to unlock my smartphone and always carry it with me, so I find it too difficult to use an item for it. But I can imagine it well with a tablet-PC or laptop."* (P2)
- *"I consider it too cumbersome to always have to carry an item."* (P10)

28% stated that they would not like to use it at the moment because the concept is still in a prototype state.

- *"At the current state I can't imagine using it because it's a prototype."* (P25)

DISCUSSION AND LIMITATIONS

In this paper, we demonstrate the feasibility of 3D-Auth items and a first user study of their usability. Still, there are security-related aspects that have to be considered when developing 3D-Auth items. In the remainder of this section, we discuss the *evaluation of the 3D-Auth prototypes* before discussing *security-related aspects*.

Evaluation of 3D-Auth Prototypes

We evaluated the prototypes in a user study with 25 participants. We provided a generic two-factor authentication scenario and a smartphone. Overall, the participants could perform 80% of the interactions correctly and remembered 94% of them. The most common reason for an incorrect interaction was that the participants did not touch the conductive dots on top of the object to "activate" it. This issue could be addressed by a better introduction to the functionality of the item. Instead of providing such an introduction, we just explained the interaction but not the purpose of touching the dots.

The second most common reason was that the object was placed in a wrong orientation. This can be addressed by adding additional dots in the bottom that enable an orientation recognition, such as the recognition solution presented in [39]. In the additional questions, the participants frequently stated that the items are easy to use. This is also supported by the user experience scale perspicuity, which refers to the ease of getting familiar with a product and learning how to use it.

Security

The authentication pattern on the bottom of a 3D-Auth item is critical for its security. While our paper primarily focuses on the interactions and their usability, we provide an analysis of the authentication pattern and the security of 3D-Auth in the following.

Password Space of 3D-Auth Items

The number of the touch-points in the authentication pattern and their possible combinations form the password space of the 3D-Auth items. Many device-specific APIs of mobile devices provide access to a maximum of ten touch-points at once, one for each finger. It is furthermore often possible to recognize different sizes of the touch-points. The minimal size of a touch-point has to be 0.5 cm and the minimal distance has to be 0.5 cm. If the distance would be smaller, multiple touch-points would be recognized as one. For this analysis, we consider a Pixel 3 XL which has the measurements of 158.0 × 76.7 × 7.9 mm. Our 3D-Auth prototypes which are detailed below use an area of 4×4 cm for recognizing the authentication pattern. This is identical to the space covered by an Android unlock pattern. Considering the sizes and distances of the touch-point, 16 touch-points fit in an area of 4×4 cm. This results in $2^{16} - 1 = 65,535$ possible combinations if all touch-points have a uniform size[2].

To increase the 65,535 combinations further, an authentication pattern may also utilize capacitive raw data [39]. As such patterns usually consist of 4×4 mm cells that can be independently read out if electrically separated by neighbouring cells, a grid of 4×4 cm can encode 25 bit (i.e. $(40\text{mm}/4\text{mm}\ /2)^2$) of information ($2^{25} = 33,554,432$). In comparison, there are 389,112 valid 3×3 unlock patterns in Android [24] and 4-digit PINs have 10,000 possible combinations. This shows that 3D-Auth items have a larger password space than 4-digit PINs and unlock patterns. Note, that the password space described here is the overall password space of 3D-Auth. The password space of individual items might be smaller based on the size of the item and its configuration options. For instance, the password spaces of each 3D-Auth prototype used in the user study is smaller than the overall password space.

Dynamic Authentication Patterns

Until now, we limited our calculation to a static authentication pattern. Dynamic patterns that change based on the interaction could further increase the password space and strengthen the security of 3D-Auth. Combining different interactions would realize such a dynamic pattern. This could, for instance, be changing the configuration of a 3D-Auth item multiple times while it is placed on the touchscreen. While our work serves as a stepping stone for 3D-Auth items, future work should consider the combination of interactions and their impact on usability and security.

Attack Mitigation

There are several attacks that an adversary might execute to either obtain the authentication pattern or to impersonate the user. In this section, we discuss attacks on 3D-Auth and means to address them.

The authentication pattern is a set of touch-points. Depending on the user's interaction with the 3D-Auth item, different conductive dots are turned into touch-points such that they can be recognized by the touchscreen. One possibility would be embedding only the conductive dots that form the user's authentication pattern. From a security perspective, this can result in the following two issues: 1) the pattern would be susceptible to a shoulder-surfing attack because it is visible, and 2) if an adversary obtains a 3D-Auth item it would be easy to perform a brute-force attack by trying interactions or just building an object that embeds the pattern.

To provide shoulder-surfing resistance, i.e., an adversary cannot obtain the pattern by taking a picture of the bottom of the 3D-Auth item, the pattern has to be hidden visually or additional dots must be added. The additional dots also mitigate brute-force and copy-attacks. This is because false interactions can lead to a false pattern that can be sensed by the touchscreen. The authentication software can react to wrong authentication

[2]One is subtracted because the case of no touch-points at all cannot be recognized as authentication pattern

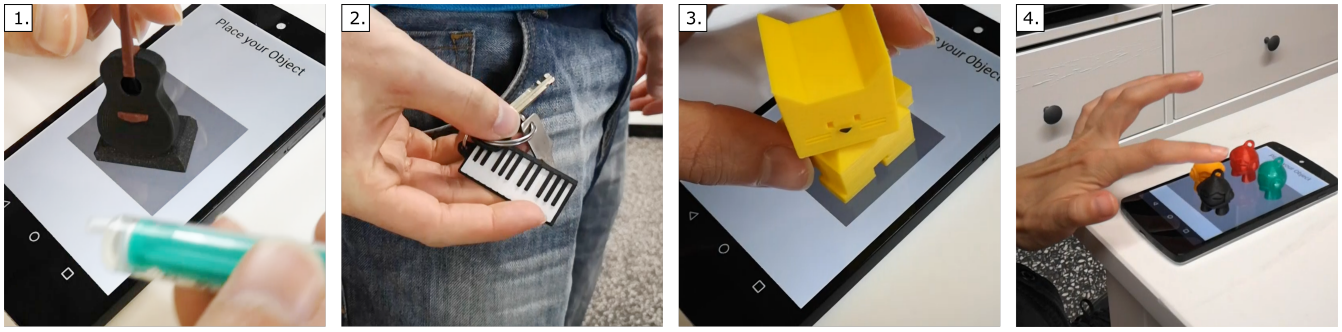


Figure 5. With the advance of 3D printing, more sophisticated items in individual shapes are possible. This could, for instance, be 1) a decorative guitar at home (augmentation), 2) a keyring (touch), 3) the shape of the favourite animal (configuration), or 4) a set of figures (arrangement).

attempts, for instance by limiting the total number of trials or reducing the number of trials by blocking authentication attempts for a certain period of time.

Furthermore, an adversary who gains full control over the device, e.g., by root access, could perform a replay attack by recording the sensor input during an authentication and replaying it later on. To mitigate this attack, we propose a challenge-response approach by using a sequence of authentication patterns. Therefore, the user receives a challenge from the authentication software asking for a specific configuration of the 3D-Auth item. The user configures the item and places it on the touchscreen. Similar to requesting the n-th transaction number in online banking, the software could request the n-th configuration of the item. Since each sequence of configurations is different, the replay attack is mitigated.

OUTLOOK

In this section, we provide an outlook how more sophisticated 3D-Auth items could be and how they could be used in the future. Furthermore, we provide directions for future work.

In our study, we have used items with simple shapes and of similar sizes. More sophisticated items can be smaller while at the same time increasing their password space as compared to the analysed prototypes because advances in 3D printing will enable more precise prints. More sophisticated 3D-Auth items could also be in a shape that is customized based on the user's preference. This could be the user's favourite animal, or other shapes that they like. Furthermore, 3D-Auth interactions could be integrated into everyday objects, such as accessories, keyrings, or other items that users carry in their wallet (see Figure 5 for examples).

While we propose 3D-Auth items as a standalone authentication mechanism, they can also be leveraged to supplement other authentication mechanisms. The second authentication factor of the 3D-Auth items is the knowledge of the interaction. In all studies, the experts and users also considered items that are based on the encoding only. While this reduces security, it might be a viable solution for use cases where the item can be stowed away in a secure space. The item could then be used for rare interactions, such as the PUK or PIN2 numbers of a SIM card. It could also be used to add a second authentication factor to an existing authentication scheme, such as the combination of a 3D-Auth item and a password. Furthermore, the 3D-Auth items could serve as an interface that is shared by different users. In this case, the factor of ownership is reduced and each user has an individual sequence of interactions for authentication. Users that are in the same environment might share a set of 3D-Auth items. The interaction category of assembly might be leveraged to provide a group-based authentication. The different parts of the item could be distributed to different members of the group that have to put the parts together.

In our study, we chose to investigate simple items that only provide one possible interaction. Combining multiple interactions to a dynamic authentication pattern results in enhanced security and therefore forms an important part of future work. The usefulness of our concept for special user groups, such as (visually) impaired people, children or the elderly, furthermore constitutes an important path for future work.

CONCLUSION

This paper presented 3D-Auth: a stepping stone towards a novel concept for enabling two-factor authentication on touchscreens. We contribute an interaction space with five categories of interaction concepts that we identified through expert design studies. These categories are: touch, arrangement, assembly, configuration, and augmentation. We realized one proof-of-concept prototype for each category. Through a user study with 25 participants, we demonstrated the usability and memorability of the 3D-Auth items. As a next step, more sophisticated items that combine several interactions should be designed and investigated in terms of usability and security.

ACKNOWLEDGMENTS

This research work has been funded by the Horst Görtz Foundation, by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – 251805230/GRK 2050; 326979514/3DIA) and JST CREST Grant No. JPMJCR16E1 Experiential Supplements. Furthermore, this research work has been funded by the German Federal Ministry of Education and Research and the Hesse State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity. The authors would furthermore like to thank Marco Fendrich for 3D-printing the prototypes for the user study.

REFERENCES

[1] Bernd Bickel, Moritz Bächer, Miguel a. Otaduy, Hyunho Richard Lee, Hanspeter Pfister, Markus Gross, and Wojciech Matusik. 2010. Design and Fabrication of Materials with Desired Deformation Behavior. *ACM Transactions on Graphics* 29, 4 (July 2010), 1. DOI: http://dx.doi.org/10.1145/1833351.1778800

[2] Joseph Bonneau, Cormac Herley, Paul C. Van Oorschot, and Frank Stajano. 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE, Piscataway, NJ, USA, 553–567. DOI: http://dx.doi.org/10.1109/SP.2012.44

[3] Eric Brockmeyer, Ivan Poupyrev, and Scott Hudson. 2013. PAPILLON: Designing Curved Display Surfaces with Printed Optics. In *Proceedings of the Symposium on User Interface Software and Technology (UIST '13)*. ACM, New York, NY, USA, 457–462. DOI: http://dx.doi.org/10.1145/2501988.2502027

[4] Jesse Burstyn, Nicholas Fellion, and Paul Strohmeier. 2015. *PrintPut: Resistive and Capacitive Input Widgets for Interactive 3D Prints*. Vol. 9296. Springer, Cham, Switzerland. DOI: http://dx.doi.org/10.1007/978-3-319-22701-6 Series Title: Lecture Notes in Computer Science Publication Title: INTERACT 2015.

[5] Elie Bursztein. 2018. The Bleak Picture of Two-Factor Authentication Adoption in the Wild. https://elie.net/blog/security/ the-bleak-picture-of-two-factor- authentication-adoption-in-the-wild/. (2018). [Online; accessed: 22-August-2019].

[6] Swati Chaudhari, SS Tomar, and Anil Rawat. 2011. Design, Implementation and Analysis of Multi Layer, Multi Factor Authentication (MFA) Setup for Webmail Access in Multi Trust Networks. In *Proceedings of the International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*. IEEE, Piscataway, NJ, USA, 27–32.

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

[8] Stéphane Ciolino, Simon Parkin, and Paul Dunphy. 2019. Of Two Minds about Two-Factor: Understanding Everyday FIDO U2F Usability through Device Comparison and Experience Sampling. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, US, 339–356. https://www.usenix.org/conference/soups2019/presentation/ciolino

[9] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. 2018. "It's Not Actually That Horrible": Exploring Adoption of Two-Factor Authentication at a University. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 456, 11 pages. DOI: http://dx.doi.org/10.1145/3173574.3174030

[10] Federal Financial Institutions Examination Council. 2005. Authentication in an Internet Banking Environment. *Retrieved June* 28 (2005), 2006.

[11] Sanchari Das, Andrew Dingman, and L. Jean Camp. 2018. Why Johnny Doesn't Use Two Factor a Two-Phase Usability Study of the Fido u2f Security Key. In *Proceedings of the International Conference on Financial Cryptography and Data Security (FC)*. Springer, Cham, Switzerland, 1–20. DOI: http://dx.doi.org/10.1007/978-3-662-58387-6_9

[12] Sanchari Das, Bingxing Wang, Zachary Tingle, and L Jean Camp. 2019. Evaluating User Perception of Multi-Factor Authentication: A Systematic Review. *arXiv preprint arXiv:1908.05901* (2019).

[13] Emiliano De Cristofaro, Honglu Du, Julien Freudiger, and Greg Norcie. 2013. A Comparative Usability Study of Two-Factor Authentication. *arXiv preprint arXiv:1309.5344* (2013).

[14] Lada Gorlenko and Roland Merrick. 2003. No Wires Attached: Usability Challenges in the Connected Mobile World. *IBM Systems Journal* 42, 4 (2003), 639–651. DOI:http://dx.doi.org/10.1147/sj.424.0639

[15] Paul A. Grassi, James L. Fenton, and Michael E. Garcia. 2017. *Digital Identity Guidelines [Including Updates as of 12-01-2017]*. Technical Report. NIST Special Publication 800-63-3.

[16] Nancie Gunson, Diarmid Marshall, Hazel Morton, and Mervyn Jack. 2011. User Perceptions of Security and Usability of Single-Factor and Two-Factor Authentication in Automated Telephone Banking. *Computers & Security* 30, 4 (2011), 208–220.

[17] Jonathan Hook, Thomas Nappey, Steve Hodges, Peter Wright, and Patrick Olivier. 2014. Making 3D Printed Objects Interactive Using Wireless Accelerometers. In *Proceedings of the Extended Abstracts of the Conference on Human Factors in Computing Systems (CHI EA '14)*. ACM, New York, NY, USA, 1435–1440. DOI: http://dx.doi.org/10.1145/2559206.2581137

[18] Scott E. Hudson. 2014. Printing Teddy Bears: A Technique for 3D Printing of Soft Interactive Objects. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 459–468. DOI: http://dx.doi.org/10.1145/2556288.2557338

[19] Yoshio Ishiguro and Ivan Poupyrev. 2014. 3D Printed Interactive Speakers. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 1733–1742. DOI:http://dx.doi.org/10.1145/2556288.2557046

[20] Kunihiro Kato and Homei Miyashita. 2016. 3D Printed Physical Interfaces That Can Extend Touch Devices. In *Proceedings of the Symposium on User Interface Software and Technology (UIST '16)*. ACM, New York, NY, USA, 47–49. DOI: http://dx.doi.org/10.1145/2984751.2985700

[21] Gierad Laput, Eric Brockmeyer, Scott E. Hudson, and Chris Harrison. 2015. Acoustruments: Passive, Acoustically-Driven, Interactive Controls for Handheld Devices. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2161–2170. DOI: http://dx.doi.org/10.1145/2702123.2702414

[22] Bettina Laugwitz, Theo Held, and Martin Schrepp. 2008. Construction and Evaluation of a User Experience Questionnaire. In *Proceedings of the HCI and Usability for Education and Work*. Springer, Berlin/Heidelberg, Germany, 63–76. DOI: http://dx.doi.org/10.1007/978-3-540-89350-9_6

[23] Simon J. Leigh, Robert J. Bradley, Christopher P. Purssell, Duncan R. Billson, and David a Hutchins. 2012. A Simple, Low-Cost Conductive Composite Material for 3D Printing of Electronic Sensors. *PLoS ONE* 7, 11 (Nov. 2012), e49365. DOI: http://dx.doi.org/10.1371/journal.pone.0049365

[24] Marte Loge, Markus Duermuth, and Lillian Rostad. 2016. On User Choice for Android Unlock Patterns. In *Proceedings of the EuroUSEC European Workshop on Usable Security*. Internet Society, Reston, VA, USA.

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

[26] Philipp Mayring. 2010. Qualitative Inhaltsanalyse. In *Handbuch qualitative Forschung in der Psychologie*. Springer, Cham, Switzerland, 601–613.

[27] Martez Mott, Thomas Donahue, G. Michael Poor, and Laura Leventhal. 2012. Leveraging Motor Learning for a Tangible Password System. In *Extended Abstracts of the CHI conference on Human Factors in Computing Systems (CHI EA '12)*. ACM, New York, NY, USA, 2597–2602. DOI: http://dx.doi.org/10.1145/2212776.2223842

[28] Jakob Nielsen. 1992. Finding Usability Problems Through Heuristic Evaluation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 373–380. DOI: http://dx.doi.org/10.1145/142750.142834

[29] Makoto Ono, Buntarou Shizuki, and Jiro Tanaka. 2013. Touch & Activate: Adding Interactivity to Existing Objects Using Active Acoustic Sensing. In *Proceedings of the Symposium on User Interface Software and Technology (UIST '13)*. ACM, New York, NY, USA, 31–40. DOI:http://dx.doi.org/10.1145/2501988.2501989

[30] Julian Panetta, Qingnan Zhou, Luigi Malomo, Nico Pietroni, Paolo Cignoni, and Denis Zorin. 2015. Elastic Textures for Additive Fabrication. *ACM Transactions on Graphics* 34, 4 (2015), 135:1–135:12. DOI: http://dx.doi.org/10.1145/2766937

[31] Jesús Pérez, Bernhard Thomaszewski, Stelian Coros, Bernd Bickel, José A. Canabal, Robert Sumner, and Miguel A. Otaduy. 2015. Design and Fabrication of Flexible Rod Meshes. *ACM Transactions on Graphics* 34, 4 (July 2015), 138:1–138:12. DOI: http://dx.doi.org/10.1145/2766998

[32] Thanasis Petsas, Giorgos Tsirantonakis, Elias Athanasopoulos, and Sotiris Ioannidis. 2015. Two-factor Authentication: Is the World Ready?: Quantifying 2FA Adoption. In *Proceedings of the EuroSec European Workshop on System Security (EuroSec '15)*. ACM, New York, NY, USA, Article 4, 7 pages. DOI: http://dx.doi.org/10.1145/2751323.2751327

[33] Munehiko Sato, Ivan Poupyrev, and Chris Harrison. 2012. Touché: Enhancing Touch Interaction on Humans, Screens, Liquids, and Everyday Objects. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. ACM, New York, NY, USA, 483. DOI: http://dx.doi.org/10.1145/2207676.2207743

[34] Valkyrie Savage, Colin Chang, and Björn Hartmann. 2013. Sauron: Embedded Single-Camera Sensing of Printed Physical User Interfaces. In *Proceedings of the Symposium on User Interface Software and Technology (UIST '13)*. ACM, New York, NY, USA, 447–456. DOI: http://dx.doi.org/10.1145/2501988.2501992

[35] Valkyrie Savage, Ryan Schmidt, Tovi Grossman, George Fitzmaurice, and Björn Hartmann. 2014. A Series of Tubes: Adding Interactivity to 3D Prints Using Internal Pipes. In *Proceedings of the Symposium on User Interface Software and Technology (UIST '14)*. ACM, New York, NY, USA, 3–12. DOI: http://dx.doi.org/10.1145/2642918.2647374

[36] Martin Schmitz, Martin Herbers, Niloofar Dezfuli, Sebastian Günther, and Max Mühlhäuser. 2018. Off-Line Sensing: Memorizing Interactions in Passive 3D-Printed Objects. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 182, 8 pages. DOI:http://dx.doi.org/10.1145/3173574.3173756

[37] 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 Symposium on User Interface Software & Technology (UIST '15)*. ACM, New York, NY, USA, 253–258. DOI: http://dx.doi.org/10.1145/2807442.2807503

[38] Martin Schmitz, Andreas Leister, Niloofar Dezfuli, Jan Riemann, Florian Müller, and Max Mühlhäuser. 2016. Liquido: Embedding Liquids into 3D Printed Objects to Sense Tilting and Motion. In *Proceedings of the CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. ACM, New York, NY, USA, 2688–2696. DOI: http://dx.doi.org/10.1145/2851581.2892275

[39] Martin Schmitz, Jürgen Steimle, Jochen Huber, Niloofar Dezfuli, and Max Mühlhäuser. 2017. Flexibles: Deformation-Aware 3D-Printed Tangibles for Capacitive Touchscreens. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 1001–1014. DOI: http://dx.doi.org/10.1145/3025453.3025663

[40] Martin Schmitz, Martin Stitz, Florian Müller, Markus Funk, and Max Mühlhäuser. 2019. ./Trilaterate: A Fabrication Pipeline to Design and 3D Print Hover-, Touch-, and Force-Sensitive Objects. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, USA, Article 454, 13 pages. DOI: http://dx.doi.org/10.1145/3290605.3300684

[41] Christian Schumacher, Bernd Bickel, Jan Rys, Steve Marschner, Chiara Daraio, and Markus Gross. 2015. Microstructures to Control Elasticity in 3D Printing. *ACM Transactions on Graphics* 34, 4 (July 2015), 136:1–136:13. DOI:http://dx.doi.org/10.1145/2766926

[42] DUO Security. 2019. Security Tokens. https://duo.com/product/trusted-users/two-factor-authentication/authentication-methods/security-tokens. (2019). [Online; accessed: 22-August-2019].

[43] International Organization For Standardization. 1998. ISO 9241-11: Ergonomics of Human System Interaction – Part 11: Guidance on Usability. (1998).

[44] Statista. 2018. Cybersecurity & Cloud 2018. (August 2018). https://de.statista.com/statistik/studie/id/58204/dokument/cybersecurity-und-cloud/ (accessed 16 September 2019).

[45] Elizabeth Stobert and Robert Biddle. 2014. The Password Life Cycle: User Behaviour in Managing Passwords. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, US, 243–255.

[46] 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 *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, US, 123–140.

[47] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. 2016. Understanding Password Choices: How Frequently Entered Passwords Are Re-used Across Websites. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, US, 175–188.

[48] Jake Weidman and Jens Grossklags. 2017. I Like It, but I Hate It: Employee Perceptions Towards an Institutional Transition to BYOD Second-Factor Authentication. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC 2017)*. ACM, New York, NY, USA, 212–224. DOI: http://dx.doi.org/10.1145/3134600.3134629

[49] Catherine S. Weir, Gary Douglas, Martin Carruthers, and Mervyn Jack. 2009. User Perceptions of Security, Convenience and Usability for Ebanking Authentication Tokens. *Computers & Security* 28, 1-2 (2009), 47–62. DOI:http://dx.doi.org/10.1016/j.cose.2008.09.008

[50] Karl Willis, Eric Brockmeyer, Scott Hudson, and Ivan Poupyrev. 2012. Printed Optics: 3D Printing of Embedded Optical Elements for Interactive Devices *(UIST '12)*. ACM, New York, NY, USA, 589. DOI: http://dx.doi.org/10.1145/2380116.2380190