University of Glasgow | School of Computing Science

Honours Individual Project Dissertation

Tangible 2-Factor Authentication

Designing and Investigating Authentication Objects for Daily Usage

Mark Turner

January 26, 2022

Abstract

“Two-factor authentication is already a widely used and recommended method of securing one’s data, however most of the preferred solutions tend to remain in the digital space. This project investigated the usability of tangible, 3D-printed objects that made use of a conductive form of plastic to interact with a capacitive touch screen. This paper finds whether this type of authentication can compare to existing two-factor authentication solutions by performing a week-long field study culminating in a recorded interview, having developed model designs based on user feedback as well as creation of a mock authentication app for data collection. This paper finds that, compared with other two-factor methods, while T2FA is less usable currently with the lack of feedback being cited as a major problem, it shows great promise, with participant feedback indicating a high interest level in a more developed version. With further development in this area, this could become a widespread method of authentication with a good amount of re-usability without sacrificing account security as with repeated passwords.“

Education Use Consent

I hereby grant my permission for this project to be stored, distributed and shown to other University of Glasgow students and staff for educational purposes. **Please note that you are under no obligation to sign this declaration, but doing so would help future students.**

Signature: Mark Turner Date: 26 January 2022

Contents

1 Introduction

With touchscreens becoming more ubiquitous and the devices using them requiring authentication more frequently, fast and simple methods have become the preferred way to access devices and accounts, with pins and patterns taking precedence over more secure 2-factor methods [Colnago et al. (2018), Reese et al. (2019)]. As such, the importance for a method of secure authentication that users will happily use has become greater over the years, as too many 2-factor methods are considered cumbersome and a waste of time by some users [Marky et al. (2021), Das et al. (2018)], by forcing them to jump back and forth between tabs and devices, waiting for codes to generate or requiring multiple additional devices that rely on network or battery. Something new is needed to solve these issues and improve the adoption of 2-factor authentication as a whole, allowing users to secure their account from malicious actors without sacrificing usability - a failing of contemporary methods. Even those 2FA methods developed that have been found to be more usable than passwords tend to leave users with some concerns affecting adoption rates [Ghorbani Lyastani et al. (2020)]. Tangible authentication offers a break from these problems by presenting more enjoyable method, as well as being more open to the addition of customisation [Sherman et al. (2014)].

This project presents Tangible 2-Factor Authentication (T2FA), a simple method of 2-factor authentication using a physical, 3D-printed model and a capacitive touchscreen device to authenticate a user through ownership of the object and the knowledge of how to use it. The object, using an interaction space previously defined by Marky et al. (2020), takes the form of a small, everyday object with touch points encoded in the model's structure made from a conductive plastic that interpret the user's interaction with the model and convey it onto their touchscreen device to authenticate.

Previously, 3D printed objects have been shown to work in lab studies, however these studies have not used realistic dimensions, as a result, performance under daily usage is unclear. This work fills this gap by creating a group of models based on user feedback, with the three most suitable being selected for use in a long-form field study. This study aimed to specifically investigate the usability of the authentication method in this way by introducing it into potential users' daily routines. To facilitate this, an Android app was built for users to perform mock authentications with their assigned model during the study, as well as to collect data on their use.

This project saw a preliminary study carried out, with one participant selected for each of the models and asked to perform authentications throughout their day for a week and return to feedback on their experiences, results of which indicated that while the method proved to be less usable than other contemporary 2-factor methods with data indicating a lower average SUS score, the participants were each eager to welcome tangible two-factor authentication in the future as an alternative to other contemporary methods.

Hence, while it certainly requires further development to improve on consistency of interaction reads and better methods of tracking ownership, T2FA shows great promise in becoming a new method of two-factor authentication, offering a break from purely digital methods with a more fun and concrete interaction which this paper found to be important to users, allowing for users to take security into their own hands.

The remainder of this paper is structured as follows:

- Chapter 2 introduces the background information required to fully understand this project
- Chapter 3 outlines previous work done in related areas that this work draws on
- Chapter 4 details the concept of the paper and what was carried out
- Chapter 5 outlines the evaluation methodology and obtained results from a usability study performed
- Chapter 6 is a discussion of the results found as well as potential implications of this work
- Chapter 7 concludes the work
- Chapter 8 gives acknowledgements to those that helped

2 Background

To fully understand the work presented, relevant areas have been outlined to ensure a base level of knowledge. In particular, this section will discuss *two-factor authentication in a general sense, 3D-Auth, 3D printing and object recognition*, and *technical details*.

2.1 Two-Factor Authentication

Authentication can be performed through three different methods, or factors - these being knowledge, ownership and inherence. Passwords are the most widely used method of authentication, being knowledge based, however, these tend to have security issues surrounding their weak nature due to reuse or simplicity and in some cases how they are stored by service providers being vulnerable to attack [Stobert and Biddle (2014), Ur et al. (2015)], leading to less secure accounts. Two-factor authentication expands authentication further, adding another required check before verifying access, a widely used example of which are bank cards, which use a knowledge based pin and a personal card as an ownership check. In the case of T2FA, these two factors mirror the example given, with a knowledge and ownership factor.

2.2 3D-Auth

3D-Auth [Marky et al. (2020)] described the use of 3D printed models for tangible authentication, outlining different methods of interaction (such as touching a specific part of an object or assembling multiple models in a certain way) after performing a design study with experts from different areas. The paper built prototypes for each of these interaction types and assessed them in a lab study to find how usable and memorable the methods of interaction were. The prototypes were created using 3D printing of conductive and non-conductive materials designed in such a way that interactions could be read by a capacitive touch screen and validated using a smartphone app. Being prototypes, the models used in the study were bulky, with each object being large proving difficult to perform a user field study with, so this study hopes to improve on this, taking the interaction space that was defined and designing new models to assess the principle of this form of tangible authentication for daily use.

2.3 3D Printing and Object Recognition

The models have been designed to utilise conductive (cPLA) and non-conductive (PLA) filament. The basic method of interaction when using the models involves placing the object onto the touchscreen, then performing an action. Each action requires that the user touch one or more specific parts of the object, with each of these parts containing conductive material. The touches performed on the object are transmitted by internally printed conductive PLA to the capacitive sensors on the touchscreen, activating the sensors in the same way a finger would. The touches read by the screen are then interpreted by the authentication program and translated into either a pass or fail. More simply, the model acts as a middleman between user and touchscreen, turning

the user's actions with the model into a sort of pass code read by the screen, this is the knowledge factor. In addition to this, the models itself also contains a space for a 'footprint', that is, a unique series of points that would identify ownership of the model that is also read by the touchscreen - the ownership factor.

2.4 Technical Details

The models were each printed with a Prusa MK3 printer [Prusa (2022b)], with a multi-material unit attachment (MMU2.0) [Prusa (2022a)], allowing for multiple filaments to be loaded at a time when printing. This is how the internal 'wiring' was achieved. To ensure it was easy for users to find the touch points, as well as for aesthetic reasons, the non-conductive PLA was a different colour from the conductive - in the case of this study, the insulating PLA was red while the cPLA was black.

3 Related Work

In this section, previous research contributions that this work builds upon will be discussed. In particular, there are 3 relevant areas of research for this project that are detailed: *two-factor authentication, 3d printed interactive objects*, and *tangible authentication.*

3.1 Two-Factor Authentication

Many methods of authentication involving two factors have already been proposed, with some already in use by end-users on different platforms and services. Some utilise one-time passcodes which are transmitted to the user via email, SMS [Aloul et al. (2009)], or in some cases generated by a physical token [Security (2019)]. However, these often trade-off usability, resulting in low adoption rates when not mandatory due to the perceived hassle of using it - failings like SMS arriving too late come to mind. Additionally, research has been done proving the ineffectiveness of some methods of digital two-factor authentication, outlining various methods of attack exploiting them such as Trojans [Dmitrienko et al. (2014)] or phishing attacks [Markert et al. (2019)].
The reason behind low adoption rates has been investigated thoroughly. Bonneau et al. (2012) defined eight usability criteria, and found that none of the contemporary schemes analysed met all of them fully, finding them as more secure but generally less usable than traditional passwords. Additionally, Colnago et al. (2018) found that, despite a usable design, some users are still put off and tend not to use two factor authentication due to bias from previous experience, suggesting social influence is important in ensuring adoption, and research done by DeWitt and Kuljis (2006) showed that users valued the speed and ease with which tasks could be completed over security, indicating that the extra steps required by two-factor authentication itself tends to be cumbersome for users. For a two factor authentication method to be widely adopted, it must be fast, easy to use and even potentially different enough from those contemporary methods already employed that users with a bias against would be willing to use it. It could indeed be said that two factor authentication has an image problem, and new methods following the paradigm should consider a change in name.

3.2 3D Printed Interactive Objects

Regarding this project, the most relevant line of research involves some method of embedding conductive material into the object, whether through the use of a conductive spray on a completed object [Ishiguro and Poupyrev (2014)] or a conductive plastic embedded into printed models for various usages [Kratz et al. (2011), Chan et al. (2012), Schmitz et al. (2021), Schmitz et al. (2018), Marky et al. (2020), Leigh et al. (2012), Kato and Miyashita (2016)] as in this project.
Another line of research has involved embedding sensors into 3D printed models to allow for interactivity. In particular, methods involving the use of capacitive [Sato et al. (2012)] or acoustic [Ono et al. (2013)] sensors to detect touch or sound, or through the use of accelerometers [Hook et al. (2014)]. This allows for more complex interactions to be registered, however it also requires additional assembly and technical knowledge, creating more overhead which this project wished to avoid.

Other research has produced methods of fabricating interactive elements in other ways via digital pipelines, such as those involving optical elements [Brockmeyer et al. (2013), Willis et al. (2012)] or filling pipes with other media [Savage et al. (2014)], to create highly customizable interactive devices. In addition to this, materials have been used for the creation of flexible [Schmitz et al. (2017)] or soft [Peng et al. (2015)] objects, allowing for deformations as an interaction method.

3.3 Tangible Authentication

Multiple different approaches have been outlined in research for dealing with tangible authentication. One such method is TwistIn [Leung et al. (2018)], which utilises the sensing information in smart devices to detect simple twist gestures which are then co-analysed with the same information from the user's smart-watch to perform authentications with an accuracy of 95%, however this method is limited for use only in small, handheld devices.
Another method is the Phone Lock system [Bianchi et al. (2010)], which uses audio or haptic feedback to indicate to the user the PIN they require to authenticate, creating an interaction safe against shoulder surfing. The study performed found that the mean error rate was 7% and average authentication time for 4 PIN authentication was 13.5 seconds, deeming the results very promising, and demonstrating that secure authentication methods need not sacrifice usability heavily. Other devices utilise wearable tokens [Chen and Sinclair (2008)] or RFID [Klompmaker et al. (2012)] to verify the identity of users.

4 Concept

In this section, the development of the project will be discussed, outlining the initial requirements decided upon, issues that were found, and the final designs used in the user field study.

4.1 Initial Investigation

The initial goal of the project was to investigate the long-term interactions between users and tangible objects for authentication, in particular, objects that follow the paradigm laid out by Marky et al. (2020). Since the objects used in the lab study performed were prototypes simply demonstrating the methods of interaction, new objects would have to be made that followed the same method but took on a more desirable form for users. To that end, an existing online survey investigating the perceptions of this type of authentication among the general populace, as well as finding desirable traits that could be adapted for use in an 'alpha' version of this system of tangible two factor authentication served as a basis for this project.

4.1.1 Survey Analysis Method

To begin the analysis of the data set, it was initially filtered by four understanding questions, to ensure that participants read and comprehended the contents of the survey. This reduced the number of respondents to 88 valid responses. The relevant criteria investigated for this project were each open text questions, requiring manual investigation and categorisation. The method for categorisation of the responses will be outlined, and the tables created through the analysis can be found in Appendices Section B.

In investigating the shapes of objects that were most desired, inductive categorisation was used to generalise answers. The results collected on Table B.2 found that respondents most preferred a cube-shaped design, with other common responses being credit card-shaped and coin-shaped.

Additionally, the size most desired for these objects were collected. In cases where the respondent provided a range, the lower number was chosen, and all sizes were recorded as centimeters. In Table B.1, it can be seen most respondents fell in the range of 5 to 10 centimeters, but more generally, users clearly opt for smaller sizes, reasoning *'[so] it is portable'* (P251) and *'bigger than that is excessive'* (P286).

4.2 Creation of Final Models and Authentication App

Having obtained data on desirable qualities of such objects from the online survey analysis, prior to performing the field study two more areas would have to completed: creation of the objects to be assessed and creation of a mock authentication app. Due to the reliance both of these areas had on each other, it was decided that development should be done on them concurrently, to allow for problems to be diagnosed and dealt with quickly. Before this, however, the potential models had to be designed according to the findings.

4.2.1 Iterative Design of the objects

The process that was undertaken for designing the models began by choosing the eight most desired shapes discovered, with designs being sketched out for the following types of models: *cube, circle/coin, credit card, square, animal, necklace pendant* and *keyring*. These were chosen as they were the shapes found to be specified by multiple respondents in the analysis of the online survey, with 'phone case' being discarded from the list due to inability to plan for the size of phone participants will have, as well as 'wearable (ring)' due to the inability to plan for different participant ring sizes. Following this, multiple interaction methods were considered, initially the 'Augmentation' method was the only method immediately removed from consideration due to the requirement of external material being unfeasible for objects in the field study which should remain usable everywhere, as well as already being found to be the least usable method in the previous lab study.

The initial designs were created keeping in mind the existing constraints in place due to the 3D printing required. Each of the models was to be created with hard plastic, so no flexibility could be integrated into the designs. In addition, the models were to be designed as simply as possible, in an attempt to remove the need for any support structures during printing or extra alteration to the models after printing such as excessive sanding. Additionally, in the initial stages of design, the footprint was represented as a square touch point on some models which could be used to implement a QR-code-like footprint, while others used the combination of activated points to serve as the footprint.

The interactions initially designed for each of the models were as follows:

- **Cube** - The repeated mention of dice in the online survey inspired a touch type interaction where a user would touch a different face of the cube on the screen, with each face holding a number of conductive pips like a playing die, acting as a PIN entry with one of a side of the cube designated for use as the footprint, with a different orientation of pips to facilitate this.
- **Circle/coin** - The interaction chosen here was arrangement, with users expected to place the object on the screen and move it along a specific path while touching the conductive footprint of the object.
- **Credit card** - A touch type interaction was chosen for this object, with the idea mimicking a rotating safe mechanism where a user was to slide their finger in a circular motion over a number of touch points, then touch the final 'enter' touch point which would hold the footprint of the object.
- **Square** - This object was to take the form of multiple small squares for an arrangement interaction where users placed the different squares on the screen in a certain pattern. Once the squares had been arranged, the user was to touch any of the touch points, which would activate all of them in via conductive material exposed at the side of each square. Each square was designed with a different shape as the touch point, with one square reserved for the footprint.
- **Animal** - This object was to be an arrangement interaction, with a rotating head that required users to pose the animal in a certain way before touching exposed conductive material on the head. Depending on the pose, different points would be activated, where only the correct pose activates all of them. The footprint would be found on one of the feet of the animal. This model was uniquely left unspecified in the design stage as it was decided that an open-source model should be adapted for this purpose.
- **Necklace Pendant** - Hereafter referred to as the pendant object, this adapted the configuration prototype model - a combination lock. The model was split into four parts rather than three, with the internal axis made separate to allow for a more permanent assembly. A loop for connection to a necklace was added to the new axis, and the footprint was planned to be expressed by the bottom layer, with a unique pattern of dots to be activated on correct

use. To authentication, users were to spin each layer to enter a set combination, then touch two points on the top of the model.

- **Keyring** - This was designed as an assembly object, with three separate squares with individual loops that could be attached to a keyring. To interact, the users were to stack each object on top of one another with the bottom object on the screen, then touch the point on the top of the stacked models, with the configuration of activated points representing the footprint of the object.

Once this was complete, draft production sketches were created [C] to facilitate easier production of the digital models, as well as to reason whether the potential sizes of the object could function with the conductive material. Regarding sizes, each of these were initially only considered with respect to the finding of the survey, however it became clear that for 3D printing further considerations had to be made. Multiple sources were referenced to complete the designs, with the distance between concurrently active touch points being 4 millimeters at minimum [Schmitz et al. (2021)], the minimum thickness of models [Fictiv (2021)] and of specifically non-conductive PLA [Schmitz et al. (2015)].

In addition to the method of interaction, considerations had to be made on how to implement a 'footprint', that is, a portion of the model that could be altered to be unique for each user. It was decided that this could be indicated by the use of two dots that would activate concurrently through internal wiring.

Having designed the objects for use in the study, the creation of both the mock authentication app and the final physical models followed.

4.2.2 Final Physical Models

With the designs for the models complete, work was done creating digital versions according to the drawings, however a first pass was done through the models removing those that would prove to be too complex, as well as considering the results of the '3D Auth' [Marky et al. (2020)] lab study, cross-referencing the interaction space of each designed model with the perceived usability found in the paper, resulting in only those models using the touch, configuration or arrangement being considered for the user field study, as assembly would prove to be too cumbersome due to requiring multiple separate objects. This narrowed the number of models for consideration down to six, with the *keyring* object being removed.

Upon narrowing of the number of models to be digitized, first 'drafts' were created for each of the models digitally, with preliminary prints of the most general objects - this was to test if that app could detect multiple touch points consistently by using an in-development version of the final study app, which was altered to display touch information in the system output log. It was found that more often than not, it was unable to register the touch point separately, which upon further inspection revealed two problems: either the touch points were too close together, or the thickness of the non-conductive material was not enough to completely block touches from being registered through the model. The former problem relied on the capacitive resolution of the touch screen, while the latter on the sensitivity of the capacitive sensors in the screen. In essence, the minimum sizes derived from the prior research when designing the models proved to be too small to work consistently.

With this knowledge, a size of 5 millimeters between touch points was found to be the new minimum distance between touch points through trial and error, and the Capricate paper [Schmitz et al. (2015)] was re-examined to increase the minimum thicknesses of insulating plastic sections to 3 millimeters. A further pass was done through the models to increase these sizes where required to ensure the interaction was detected as expected.

At this point, the limitations discussed in Subsection 4.2.3 were discovered, and the decision was made to choose one 'candidate' model for each of the remaining interaction categories, taking

into account any object that may need one of the methods that were found to be unsuitable, resulting in the three final models to be taken forward into the user study: *the cube, the credit card* and *the pendant*. The design of these models is specified finally as follows:

Cube model
Evaluation of the responses from the survey indicated that the most popular shape for a tangible authentication item was a cube, with many of the responses requesting a dice model. As such, this object was designed as a die [Figure 4.1], with each of the pips on each side cPLA connected internally to each other, such that a user could touch any of the pips and activate any side. The interaction space chosen for this was arrangement, with users expected to 'stamp' a selection of the sides on the touch screen to perform an authentication, in a similar way to using a PIN. The PIN of the object was set as 4142 for the study, however the idea behind this model allows for any PIN to be set with any number of digits, as a result, the password space is potentially limitless, but assuming a PIN of four there would be 126 potential combinations (six sides to choose from, four digits needed). The footprint of this model was demonstrated on the two pip side, with two variations of the model created to display this, however due to the nature of the authentication only requiring the number of pips on the screen at once, the footprint could be implemented on any of the sides, as a variation of the positioning of each of the individual pips.

Card model
The second of the highly suggested model shapes was a flat bank card-like shape, which this model implemented, with the dimension of a credit card used for reference in its design [Figure 4.1]. The interaction space chosen for this was touch, with users asked to touch certain points of the card in order, then touch a final 'confirmation' point, which held the footprint of the card (again represented as two points of cPLA). More specifically, the interaction was designed with a safe dial lock in mind, leading to an interaction involving the user swiping their finger in a circular motion over cPLA 'dots' of material to specific points while the model rested on the touch screen [D]. The authentication app collected the locations of each of the dots and upon detecting the footprint, translated the touch data into a numerical PIN derived from how many dots were touched before swiping in the opposite direction – for example, starting from the top dot and turning clockwise to the third, then anti-clockwise would register the clockwise movement as 3. Once again, due to the method of interaction, this password space is also potentially limitless, as well as offering other methods of interaction (such as drawing a shape on the surface of the card which touched a subset of the dots), hence this object proved to be the most secure of all of the designed objects.

Pendant model
The third requested shape for the objects was something wearable, such as a ring or a necklace pendant, which this model adapted. The model could also be considered for use on a key ring. As a result of its shape, this object was designed to be the most portable and easiest to remember as it could be attached to something with which a habit of picking up had already been built. The interaction space for this object was chosen to be configuration and implemented as a small combination lock [Figure 4.1], with a loop on the central axis for attaching to a key ring, necklace, etc. Users were to move different levels of the object to complete a combination (which for the study was set at 123), then place the object on the device's screen and touch two conductive points on the top of the model. The central axis conductive point would activate regardless of the correctness of the configuration, while the outer point only activated if the configuration was correct, and led to the footprint of the object which was implemented as two dots. Assuming ten parts of the bottom surface, the footprint would be represented by certain parts of the bottom surface activating – in this case, it was the parts linked to the numbers two and four. Each level of the combination lock design offered 10 possible options, leading to 120 possible combinations, which could be increased by adding further layers or more options per layer.

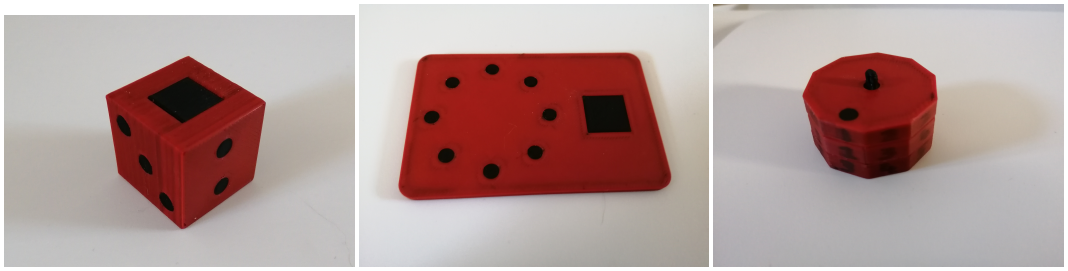


Figure 4.1: *The 3 models used in the study, the cube model (left), the card model (center) and the pendant model (right).*

4.2.3 Mock Authentication App

A mock authentication app was required for this study to provide the participants somewhere to use their given object for authentication and mimic the need for authentication throughout the day by sending notifications. This also served to collect some data that would be useful in determining the usability of the authentication method.

The first task when creating the app was to define the list of initial requirements, as well as the platforms to build for. The app was decided to be created for Android in Java, as it was felt this would allow for the largest number of people to participate in the study, considered the simplest and most versatile to develop for, as well as already having access to the Google Play Store meaning it would be easy to install for participants. The requirements generated indicated there was a small amount of functionality that had to be implemented to be considered complete:

- The app must be able to send notifications multiple times per day to remind users to authenticate, simulating the need for authentication throughout the day.
- The app must be able to register the authentication attempts made by the users.
- The app must be able to collect data on the authentication attempts and save to a log file for retrieval of the collected data at the end of the user study.

As well as this, it had to be decided what data to collect during the authentication attempts, the final list of data collected being *participant number and model provided, when the authentication attempt took place, whether the authentication was a success, the number of attempts it took, how long it took*, as well as *a user input indicating where they were when they authenticated.*

The app was created a built to meet each of the requirements one by one, with notifications being dealt with first: using a random number generator the interval until the next notification was set upon opening the app (resulting in only one notification at a time) then scheduled to be sent using Android's Alarm Manager package. In addition, notification were specified to only be sent during the hours of 8a.m. and 9p.m., ensuring that they are only received during the day, achieved by checking if the random notification delay generated fell between these hours and setting the delay to reflect this constraint. This was followed by logging of the required data which was extracted into a utility function class, both of which proved to be no issue. However, this gave rise to new requirements for the application: the app must provide a method to save the log file into accessible storage on the device (e.g. the /downloads folder); the app should provide a way to test the functionality of all implemented methods (e.g. notifications, saving the log file); the app should provide a way to change the authentication model without having to reinstall the app completely (to facilitate the 3rd stage of the exit interview).

Implementation of the app proved to be complex, as some of the methods required for use in authentication validation worked inconsistently across different devices and Android versions, returning blank or unhelpful data from essential functions, in particular the following functions:

```
MotionEvent.getHistoricalPointerCoords()
MotionEvent.getSize()
```

Since the app was to be deployed on potentially many different Android smartphones during the field study (as participants were to be asked to use their own mobile devices), it had to be built such that authentications could take place on any device running Android, meaning these methods could not be used. As a result, the authentications were limited to using the number of touchpoints on the screen at once, as well as the location of the touch points, the impact of which will be discussed in Subsection 4.2.2. This was not the only method of validation investigated for use, with the use of raw capacitive data considered initially, as used in ItsyBits [Schmitz et al. (2021)], however this proved to also be an issue, as accessing raw capacitive data on Androids required root access, which was deemed to be too invasive to use during the field study.

The final implementation utilised views to capture touch actions and upon detecting a MotionEvent.ACTION_UP, the data captured from ACTION_DOWN events were sent to a function in the view's encapsulating activity which checked the registered model and dealt with authentication attempts.

Each object would be required to have its own validation method, hence it was decided that each model should take the form of a class inheriting methods from a parent abstract class outlining a general authentication model. This allowed for any number of the models designed to be implemented in the app providing good scalability. The models implemented are as outlined in Subsection 4.2.2.

The app itself was built using Android Studio and tested manually using a physical Huawei PSmart 2019 running Android 9, as well as an emulated Google Pixel 2 running Android 10 and 11. A limited test bench was implemented, however it only tested the notification scheduling. All defined requirements were successfully met by the completed application and built into an APK, with a second release APK being built specifically for Android 10, due to the permissions required for writing to external memory being different from other versions, and a lack of time to completely implement the change into a single version.

5 Evaluation

In this section, the methodology of the study in the wild is discussed along with the results of the evaluation.

5.1 Methodology

To assess the usability of the models designed and the authentication method as a whole, an exploratory study was performed as outlined with three participants.

5.1.1 User Field Study

The purpose of performing the study was to assess how users interacted with the tangible authentication method in their daily lives over an extended period, hence a lab study would not have been sufficient. The study took place over one full week, consisting of an initial meeting, multiple daily mock authentications, and finally an exit meeting.

In the initial phase, participants were required to be present for an in-person meeting. The procedure of this meeting was as follows, and adheres to the BPS ethical guidelines:

- **1 - Familiarizing participants with the project.** Upon arrival, participants are greeted and informed about the concept of tangible two-factor authentication, as well as what they would be required to do over the week. To do so, an introduction script was designed to be read with the opportunity for any questions clearly indicated before agreeing to participate. Here it is also made clear what data will be collected and that it will be stored in accordance with the GDPR.
- **2 - Gathering informed consent.** Having explained the purpose behind the project, as well as what would be required of them, the participants were each asked to sign a consent form indicating they have understood what has been explained and that they agree to take part.
- **3 - Demographics survey.** Each participant is assigned a participant number and asked to fill out a demographics survey, consisting of basic demographic questions as well as a set of questions to find their affinity for technology (the contents of this survey can be found in Appendix Section E).
- **4 - Introduction to the object.** The participants were then assigned one of the three final models to use for the next week, as well as the mock authentication app installed on their mobile device. An information sheet demonstrating how to interact with the object is provided as well as a demonstration by the interviewer, and time is allotted to allow for the participants to get familiar with the object and method of interaction. Here all the methods in the app will also be checked for functionality on the device.
- **5 - Schedule final meeting.** Having received all of the necessary information and with the setup complete, the participants are asked to schedule a second meeting for the end of the study at least one week from the day, and any additional questions they have are answered before the end.

ID	Age	Gender	Country of Residence	Job	Work from Home	Two Factor	ATI
P1	26-30	Male	Scotland	Employed	Yes	Yes	4
P2	21-25	Male	Scotland	Student	Yes	Yes	4.44
P3	Under 21	Female	Scotland	Student	Yes	Yes	3.44

Table 5.1: *Demographics information for the participants collected in the initial meeting during the study.*

Upon completion of this initial phase, participants were to go about their daily lives as normal, ensuring that their designated model is with them, and checking for notifications from the app. Upon receiving a notification (or upon noticing a notification) from the app, participants were to perform an authentication, with three attempts to succeed. This would involve launching the study app, pressing the button to begin an authentication attempt, and interacting with their designated model as demonstrated in the initial meeting, then finally inputting where the authentication took place. Each of these authentications was considered to take a maximum of five minutes, and the participant was asked to perform at least two per day.

Once the week had concluded, the participant was asked to be present for another meeting previously scheduled. The procedure of this meeting was as follows:

- **1 – Re-familiarising.** The participant was greeted and reminded of the purpose of the study.
- **2 – Exit survey.** They were then asked to fill out an exit survey to gather the system usability score for the application method, as well as gather some extra information regarding the continued function of the object. During this time, data collected by the app is to be extracted from the mobile device.
- **3 – Exit interview.** Upon completion of the survey, the participants are asked to take part in a recorded interview and assured once again that the data they provide will be anonymous and recordings will be transcribed and deleted. The interview has 3 stages:
  - Stage 1 - Participants are asked questions about their week using the item
  - Stage 2 - Participants are asked about their perception of two-factor authentication in a general sense and concerning the project specifically
  - Stage 3 - A short break is taken allowing for participants to experience using the other two models, then asked their opinions on them, as well as on 3D printing in general.

  The complete script can be found in Appendix Section F. Upon completion, participants are offered a chance to ask any other questions or give their comments before leaving, as well as provided contact information for the investigator if they have any comments or questions after leaving.

5.1.2 Demographics

Recruitment for the participants was done through mailing lists as well as word-of-mouth. Each of the participants was required to be over 18 years of age, as well as own an Android phone. The final demographics information for the participants can be found in Table 5.1. Each of the participants was compensated with a £40 Amazon voucher for their time at the end of the study.

ID	Object	SUS	Mean Time (s)	SD	Success Rate (Attempt)	Success Rate (Authentication)
P1	Cube	60	8.09	3.67	15.00	38.71
P2	Card	52.5	5.16	2.68	53.66	88.00
P3	Pendant	60	5.47	3.49	23.40	61.11

Table 5.2: *Table detailing the quantitative results for each participant and model*

5.2 Results

Here results will be presented in two parts: *Qualitative data* and *quantitative data.*

5.2.1 Quantitative

Here the data collected by the application during the study is outlined, in addition to the results from the exit survey.

One of the metrics gathered by the study application measures the time taken to complete an authentication attempt. Since the overall time for the authentication was collected, this time was divided by the number of attempts taken to find an average time for each attempt across one authentication. The overall average time taken for each of the models is indicated in Table 5.2 as well as the standard deviation. The object with the overall fastest average time per attempt was the card model with 5.16 seconds per authentication (max = 15.51, min = 2.65, SD = 2.68). This is followed by the pendant model with 5.47 seconds per authentication (max = 12.29, min = 2.29, SD = 3.49). And lastly, the overall slowest average time per attempt was found in the cube model with 8.09 seconds per authentication attempt (max = 19.06, min = 2.03, SD = 3.67). The development of time taken per attempt can be seen for each of these models in Figure 5.1.

In addition to the collection of authentication time, the success rate was also measured by taking the number of successful attempts over the total number of attempts, with the highest overall success rate found with the card object (53.66%), followed by the pendant (23.4%) and the cube (15%). As well as on an attempt basis, the success rate was also measured on an authentication basis - that is, how many full authentication attempts resulted in a success, which showed again the card object had the highest success rate (88%), followed by the pendant (61.11%) and the cube (38.71%). These numbers can also be found in Table 5.2.

Finally, during the exit meeting, the users were asked to complete a survey with a section for the system usability scale. The final scores indicate the perceived usability of both the object and authentication app together, with an overall average of 57.5.

5.2.2 Qualitative

Here the findings from the exit interview will be outlined, with transcripts of the meeting being analysed via thematic analysis as outlined by Braun and Clarke (2006). This resulted in 5 main categories: *Security, How it feels to use, Method of use, 3D printing and Commercial* in addition to any recommended improvements.

Security
All of the participants in the study were familiar with the use of two-factor authentication, each citing different established methods that they had to use often, however two of the participants only used the methods when they were required to, with one (P2) saying the reason they do not often activate it is because they feel like they have nothing worth stealing.

When asked about how secure the model feels to use, two of the participants were unsure (P1, P2), with one noting that they felt vulnerable to shoulder surfing attacks. Interestingly, P2 mentioned

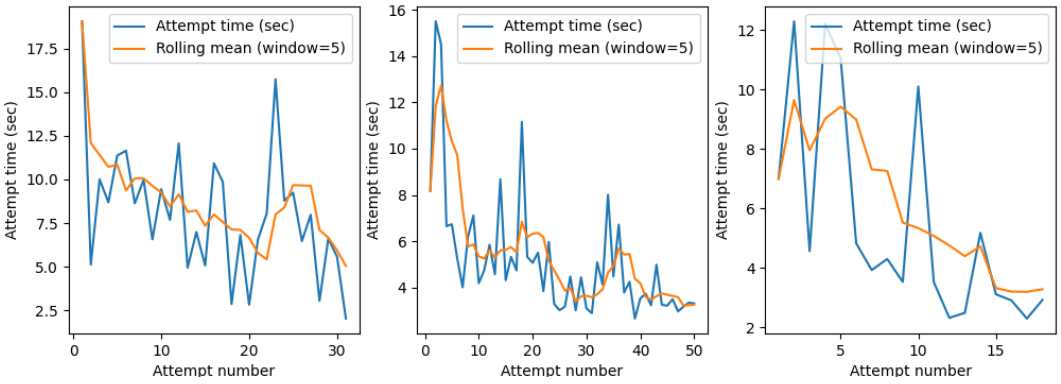


Figure 5.1: *This figure illustrates the improvement in authentication time over number of attempt for each of the 3 participants.*

that *"[they] realise how secure it is, and it is quite secure, but it doesn't necessarily feel like it."* and felt that it *"feels a bit like a toy"*.

Speaking about the physical security of the objects, two of the participants explicitly spoke about how it was unlikely for the objects to be stolen:

- *"I didn't leave the item out on a tabletop... I always carried it with me so not that much danger of it being stolen"* (P1)
- *"It would be really inconspicuous. No-one would have any idea what it is"* (P2, on the cube object)

Usability

This was the largest category that was found, linking the closest to the issue of usability during the interviews.

On the initial use of the model, two of the participants discovered a bit of a learning curve (P1, P2), with P1 mentioning they often touched the screen with their fingers during attempts at the beginning of the study. The same participants also mentioned that they felt at least one of the models was fragile, with P1 mentioning the pendant model felt fragile *"On account of it having moving parts"*, however P2 later began to feel more confident in the strength of the card model - *"I did worry about it actually breaking, but never managed to break it. You wouldn't be able to"*.

While all of the participants agreed that the model was easy to carry with them, they all disliked using them with phone in hand rather than on a tabletop or other flat surface, generally avoiding doing so. Each of them also mentioned that the models tended to slide on the phone screen, which led to failed authentications.

It was also brought up by two participants that it was felt that there was not enough feedback when authenticating, and it was difficult to tell if something went wrong, or what caused a failure. Each of the participants also felt that authenticating was inconsistent in its current state with one participant summing it up: *"Some of the time the authentication just wouldn't go through"* (P3).

Throughout it interview each of the participants also spoke about the enjoyment factor, expressing that the method was fun to use, adding to the usability, while two of the participants mentioned that the familiarity of the model and the method of interaction was also important.

Finally, each of the objects was well-liked and discussed in such as way by at least two of the participant, with the card model drawing two participants to call it their favourite, while the last preferred the cube object the most. It was also mentioned by each participant that they would prefer to use this method over other two-factor methods, with P2 adding *"at least in some scenarios"*.

Method of use
Participants were also asked about where they would prefer most to use it, and while all agree they would mainly use it for services where two-factor authentication was already implemented (systems like banking apps), there was more of a range when discussing the devices and locations. P2 stated *"I'm not sure if smart phones [are] the best place to use it"* and said they would prefer to only use it at home, so stationary devices would be best, but the other participants were willing to use the method on any device that allowed it. In terms of location however, P3 agreed is was *"definitely easier to use it at home than when I'm out."* and would prefer to use it on services they don't open a lot.

3D printing
To get a sense of how the objects could be distributed, the participants were also questioned about their opinions of 3D printing. While there was a range of answers on whether or not the participants would buy them, they all mentioned that they thought there would either be widespread adoption or in-person services available (like existing *"copy-shops"* (P1)) that would allow for printing to be done without owning a 3D printer.

Commercial
Finally, when asked if they would purchase the models for use, two of the three participants were hesitant to:

- *"I don't know... I feel it would be more used for banks"* (P3)
- *"I would consider but I don't think I would end up buying... It's more cumbersome than not at all"* (P1)

6 Discussion

In this paper, the usability of tangible two-factor authentication using conductive and insulating PLA and capacitive touch screens has been investigated. In this section, the results of the study will be discussed, along with the limitations of this paper, as well as potential future directions that may be promising for research.

6.1 Results and Improvements

The preliminary results of this study proved promising - while the objects performed inconsistently in the field due to failings in the implementation, the time taken to use them per attempt was shown to improve as the participants grew more experienced using them, with minimum times found towards the end of the study period on the order of only two seconds. This sentiment was also expressed by the users themselves, with two participants noting the learning curve during the interview section. When compared with other contemporary methods of two-factor authentication as investigated by Reese et al. (2019), we can see that in terms of timing, this method is comparable to the use of codes (mean 2.2 seconds), and far faster than more complex methods like U2F security keys (mean 57.8 seconds). Hence, it should be noted that to properly assess usability with new designs of tangible two-factor authentication objects following this paradigm, time must be allowed for users to become familiar.

Although, while this metric proved to be favourable, the success rate of authentications proved worrying, with very low rates of success per attempt. However, this was not due to a problem with the objects, or the method of interaction, as each of the participants noted that at least one of the models did not consistently authenticate in the application, despite actions being performed correctly. This was due to the capacitive resolution of the touch screen - since the models were designed with usability in mind, and respondents in the initial survey desired smaller, more portable objects, it follows that any conductive points interfacing with the touch screen would be close together because of the limited space on the object, resulting in an inconsistent read as multiple touch points are registered as one. In addition, this was affected by the implementation of the authentication app, with the issues previously discussed in Section 4.2.3 resulting in a flawed design. As a result, it can be seen that the perceived usability of the method was reduced, with a mean SUS score reflecting this, far lower than each of the methods explored by Reese et al. (2019).

Another interesting result indicated that for the more technically adept users who participated, the security of the authentication method felt more flimsy, with one participant noting the difference in expectation between their perception of security and the reality of using the item - they were aware that on paper it is secure, but due to the simplicity of using it, felt that it couldn't be secure. This brings to light a perception some users may have of two-factor security - that it must be complicated and difficult to use for it to be truly secure. This same user noted that the pendant model - the model that adapted a combination lock style of interaction - felt the most secure of the objects, despite having the solution to its interaction easily accessible by taking it apart - a potential security issue that future research in this area should consider for objects such as this one, whether by adding an extra interaction or via adding 'decoys'. This seems to indicate

that for some users, interactions should feel comparable to existing security measures for tangible authentication methods, indicating that perhaps rather than novel and enjoyable interactions, some users would prefer familiar actions that they already link with security for assurances that the method is truly secure. This disparity between user perception and reality has been noted before, such as by Zimmermann and Gerber (2020) who noted that not only can this be found in the security of a method, but also in the usability, with perceptions affected by multiple factors.

A usability issue brought up by participants was the material of the object, while strong its interaction with the phone screen resulted in difficulties for touch-based objects as the model easily slid out of place. It was suggested that a clip or some kind of holder be given alongside the object to make authentication easier, however this would create more overhead, a problem which resulted in assembly interactions being ejected from the study. While utilising a different material for the non-conductive parts of the object would increase issues with distribution, this appears to be the simplest solution to this problem and should be considered in future work.

Another trend found during the study indicated that many potential users of this authentication method preferred to keep the models for use at home with services they use rarely. As such, perhaps the focus this study had on making small and portable models was misguided, and a case could be made rather for focusing on larger, more complex models to be used solely in the home. This may also prove advantageous in the retention of users, as emphasis on portability will require users to build habits around the method, whether bringing the object with them when going outside or simply keeping it nearby, which may put some users off. At least in this current stage, it was clear the participants were not interested in using the objects more than they had to.

An improvement often mentioned by the participants involved more feedback when performing the authentication. Allowing users to see the progress they've made during the process of authentication or some form of demonstration by the app that an interaction has indeed been registered, whether via haptic feedback, or audio cues, would greatly have improved user experience during the performed study.

6.2 Limitations and Future Work

In finding the usability of the developed models, a clear limitation is the small sample size of participants drawn for the field study. As a result, the findings presented should only be considered a preliminary indication, and a follow-up study should be performed to investigate further and solidify understanding of the user experience of this concept.

One of the large issues this project faced already touched upon was the inconsistency of the model due it the study applications implementation. Over the course of development, the inconsistency of Android touch event methods was a problem, as for the implementation to be considered a success, it should run on most phones. This limited how objects could be validated, leaving the actual implementation less than secure, with only position and number of simultaneous touch points able to be used, both of which are easily replicated without the object. To truly implement this kind of authentication, this paper recommends future works instead use raw capacitive data, making use of research already done in this area such as by Schmitz et al. (2021) who used machine learning for recognition of smaller object footprints and Mayer et al. (2021) who created a method of improving the low resolution of capacitive touch screens to better detect correct interactions. Future research could consider different methods of implementing the ownership factor - rather than the positioning of two or more dots, a QR-code-like implementation could be used as Yu et al. (2011) presents.

7 Conclusion

This paper investigated the usability of a method of tangible two-factor authentication through the design and creation of models and a mock authentication app, and assessed through data from a one-week-long user field study. Preliminary user feedback indicated that despite the usability issues, willingness to adopt this method as a form of two-factor authentication was high, and while not all participants were interested in a commercially distributed form, each expressed they would welcome tangible two-factor authentication once it had matured and offered improvements they would like to see. Ultimately, the outlook on this new method of authentication provided by the preliminary field study performed suggested that this is an area in which more research should be done, and that should the problems found by this paper be solved, it could well become a widely adopted tool in the future.

8 Acknowledgements

This paper would not have been possible without the help of my colleague Laszlo Besenyei at the University of Strathclyde, who provided a great service in helping with the digital modelling of the objects, as well as Mohammed Khamis, who allowed me to intrude on his office for more than three months. I would also like to thank Karola Marky, my supervisor on this project, for lending her knowledge.

Finally, I would not have been able to complete this without the support of my wonderful fiancée, Elizabeth.

A Ethics Forms

The appendices provide the relevant ethical information as used during the evaluation. A copy of the introduction and consent sheet can be found in Figure A.1 and A.2, and the signed ethics checklist can be found in Figure A.3 and A.4.

Model Suitability Investigation
Mark Turner
2021/22

Purpose of the Study

The aim of this study is to investigate how feasible the use of 3-dimensional objects is for 2-factor authentication within daily routines. In particular, the 3D printed objects that will be used were created with user feedback in mind, so the study hopes to assess how suitable these objects are when used over a longer period of time. As such, we require a group of people to attempt to use these objects throughout their day over a period of one week to simulate having to perform 2-factor authentication to access secure apps using an app designed for this purpose.

What will I have to do?

In order to take part in this study, you must:

- Own an android phone
- Be aged 18+

If the above criteria apply to you and you give consent to participate in the study, you will be required to perform the following tasks:

- You will receive a consent form and a short demographic questionnaire, following completion of this, you will be assigned a unique participant number, a model to work with, and an app will be installed on your android phone.

- The experiment will run over the course of a week beginning today, with participants having the chance to try out using the object they have been given on their own mobile devices, which will have a custom app installed to perform the mock authentication on as well as collect some data, some of which the participant will have to provide, such as where they were when they authenticated (this will also be demonstrated today).

- Once the orientation session is complete, participants are asked to go about their normal lives, performing an authentication on the app preferably as soon as a notification is received to do so, but participants should aim for at least 2 authentications in the app per day. As such, participants should ensure to keep their model nearby to allow this to be done.

- Once the week is over, participants should come back to perform an exit interview on a day scheduled before the end of the orientation, with questions being asked about their experience using the model. After the exit interview, the participants will be compensated. The exit interview is audio recorded and before analysis, the recordings will be transcribed into written form. Personal information will be removed and replaced by neutral placeholders. The interviewer will explicitly tell you when recording has started

Data collection & use

The data that will be collected by the app automatically include the time taken to authenticate, the time of day and date the authentication took place, whether the authentication was a success and how many attempts were required. User input collected will include where the authentication took place (eg, home, work, outside etc.). Upon completion and submission, any data collected from the participants will be fully anonymous

Figure A.1: *The introduction and consent form issued during the user study. (part 1/2)*

and kept secure and password protected. The audio recordings from the exit interview will be transcribed before analysis. The data from the demographic questionnaire will be anonymised. All data from the experiment will not be linked to individuals except for the consent form.

The data will be analysed for the study and kept until past the end of the research, with the findings of the study potentially being reused in additional research projects.

Further information

During the study, should there be any problems, such as the model no longer working for any reason, wishing to drop out of the experiment, etc, the participant should contact Mark Turner by email at 2386300T@student.gla.ac.uk. If there are any problems during the orientation, I will be right here for any questions and concerns.

To be clear, this study is not assessing you in any way, but the use of the 3D models, so don't hesitate to contact me for any problems. You are free to drop out of the study at any time, however we would not be able to reimburse you, should you still choose to do so, I would ask that you get in touch so we can discuss the data collected up to that point to enable a partial reimbursement.

If you have further questions during the study, please contact:

Investigator: Mark Turner
School of Computing Science
Lilybank Gardens
2386300T@student.gla.ac.uk

Supervisor: Dr Karola Marky
School of Computing Science
Room SAWB320
karola.marky@glasgow.ac.uk

Who has reviewed this study?

This study adheres to the BPS ethical guidelines. You are free to discuss your participation in this study with the investigator or supervisor, however should you with to speak to someone not involved in this study, you may contact the chair of the School of Computing Science Ethics Committee: Prof. Matthew Chalmers.

Consent form

Please confirm to indicate that you have read the information sheet and understand the contents of the study, and that any questions you may have about the study have already been answered. You further confirm that you are 18+ years old

☐ I understand and agree to take part in this study

Name:_____ Email:_____

Signature:_____ Date:_____

Figure A.2: *The introduction and consent form issued during the user study. (part 2/2)*

Department of Computing Science
University of Glasgow

Ethics checklist form for 3rd/4th/5th year, MSc IT/CS/ACS projects

This form is only applicable for projects that use other people ('participants') for the collection of information, typically in getting comments about a system or a system design, getting information about how a system could be used, or evaluating a working system.

If no other people have been involved in the collection of information, then you do not need to complete this form.

If your evaluation does not comply with any one or more of the points below, please submit an ethics approval form to the Department Ethics Committee.

If your evaluation does comply with all the points below, please sign this form and submit it with your project.

---

1. Participants were not exposed to any risks greater than those encountered in their normal working life.
   Investigators have a responsibility to protect participants from physical and mental harm during the investigation. The risk of harm must be no greater than in ordinary life. Areas of potential risk that require ethical approval include, but are not limited to, investigations that occur outside usual laboratory areas, or that require participant mobility (e.g. walking, running, use of public transport), unusual or repetitive activity or movement, that use sensory deprivation (e.g. ear plugs or blindfolds), bright or flashing lights, loud or disorienting noises, smell, taste, vibration, or force feedback

2. The experimental materials were paper-based, or comprised software running on standard hardware.
   Participants should not be exposed to any risks associated with the use of non-standard equipment: anything other than pen-and-paper, standard PCs, mobile phones, and PDAs is considered non-standard.

3. All participants explicitly stated that they agreed to take part, and that their data could be used in the project.
   If the results of the evaluation are likely to be used beyond the term of the project (for example, the software is to be deployed, or the data is to be published), then signed consent is necessary. A separate consent form should be signed by each participant.

   Otherwise, verbal consent is sufficient, and should be explicitly requested in the introductory script.

4. No incentives were offered to the participants.
   The payment of participants must not be used to induce them to risk harm beyond that which they risk without payment in their normal lifestyle.

Figure A.3: *Signed ethics checklist. (part1/2)*

5. No information about the evaluation or materials was intentionally withheld from the participants.
   Withholding information or misleading participants is unacceptable if participants are likely to object or show unease when debriefed.

6. No participant was under the age of 16.
   Parental consent is required for participants under the age of 16.

7. No participant has an impairment that may limit their understanding or communication.
   Additional consent is required for participants with impairments.

8. Neither I nor my supervisor is in a position of authority or influence over any of the participants.
   A position of authority or influence over any participant must not be allowed to pressurise participants to take part in, or remain in, any experiment.

9. All participants were informed that they could withdraw at any time.
   All participants have the right to withdraw at any time during the investigation. They should be told this in the introductory script.

10. All participants have been informed of my contact details.
    All participants must be able to contact the investigator after the investigation. They should be given the details of both student and module co-ordinator or supervisor as part of the debriefing.

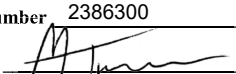
11. The evaluation was discussed with all the participants at the end of the session, and all participants had the opportunity to ask questions.
    The student must provide the participants with sufficient information in the debriefing to enable them to understand the nature of the investigation.

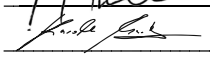
12. All the data collected from the participants is stored in an anonymous form.
    All participant data (hard-copy and soft-copy) should be stored securely, and in anonymous form.

Project title Tangible 2-Factor Authentiaction

Student's Name Mark Turner

Student's Registration Number 2386300

Student's Signature 

Supervisor's Signature 

Date 27.03.2022

Figure A.4: *Signed ethics checklist. (part2/2)*

B Online Survey Analysis

The following tables outline the findings of the analysis of the online survey performed prior to this study. After filtering for understanding, the number of valid responses numbered 88. The table of responses for size can be found in Table B.1, and for shape in Table B.2.

Size (cm)	Number of responses
1	4
2	8
3	19
4	4
5	34
6	7
7	3
8	4
10	26
12	2
13	1
15	8
20	2
30	3
45	1
50	1

Table B.1: *The number of responses for a particular size of model suggested*

Object shape	Number of responses
Cube	17
Circle/coin	13
Credit card/Rectangle	11
Square	7
Wearable (ring)	5
Animal	4
Necklace	2
Keyring	2
Phone case	2
Car key	1
Polygon	1
Cylinder	1
Fidget Spinner	1
Car	1

Table B.2: *The suggested shape of the models and the number of occurrences*

C Production Sketches

The production sketches created during development of the objects can be found in Figures C.1, C.2 and C.3

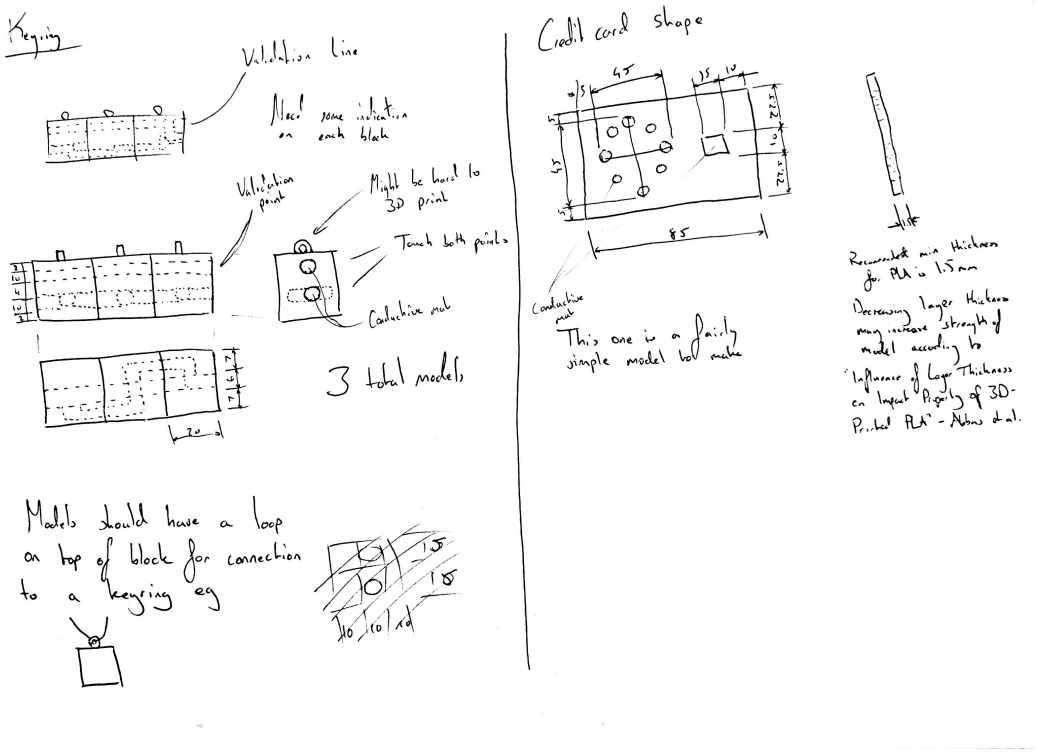


Figure C.1: *Initial production drawings for keyring and credit card models*

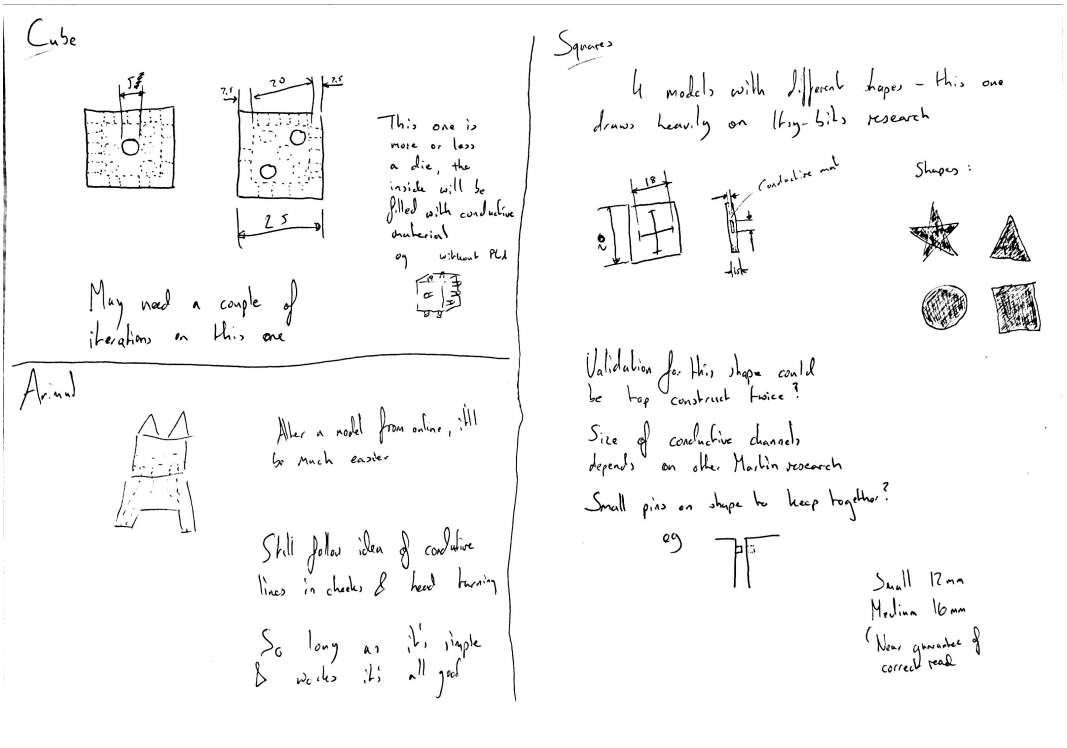


Figure C.2: *Initial production drawings for cube, animal and squares models*

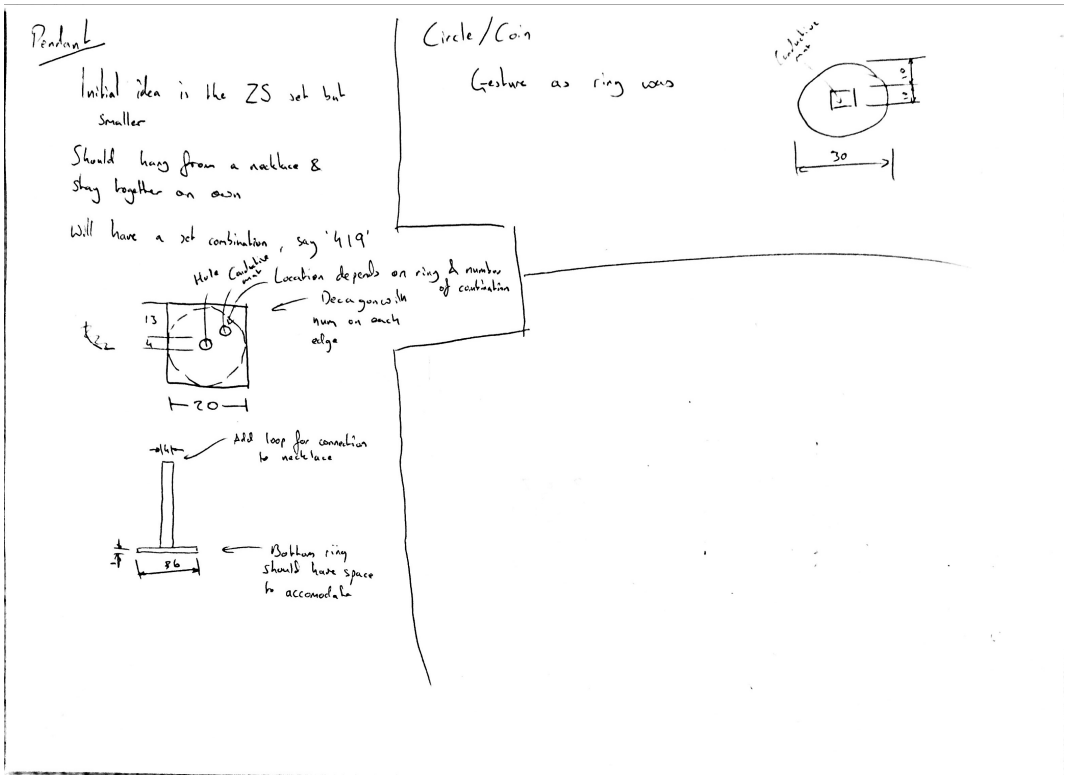


Figure C.3: *Initial production drawings for pendant and circle/coin models*

D Model Interaction Instructions

The full sheet of interaction instructions given to participants can be found in Figures D.1, D.2 and D.3.

Cube

This model is built to replicate dice, but a bit bigger, leaning in to the idea of the object being multi-use. To use this object, you must touch four of the sides to the screen in a certain pattern and the authentication will complete.

The order of the side to touch to the screen is the side showing 4 pips, then 1 pip, 4 pips and finally 2 pips. When you touch the object to the screen you must ensure that you are touching any of the black pips on any of the sides, as well as not touching the screen of the phone at any point during the authentication once you have started as this will cause the authentication to fail.

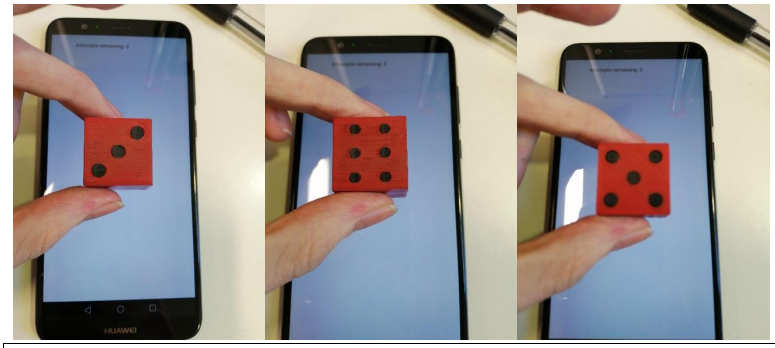


Fig. 1, Example use of the model, with 4, 1 and 2 being input (from the left). The face touching the screen determines which number is being input.

Figure D.1: *Model instructions issued to participants during the initial meeting to familiarise with assigned model. (part 1/3)*

Credit Card

This model is built to the standard size of a credit card (with some added thickness to ensure the plastic doesn't break) meaning it can fit in a wallet or purse. To use the model, you must enact a 'turning' motion over the ring of dots much like you would turn a safe lock, with the model on your phone as shown.

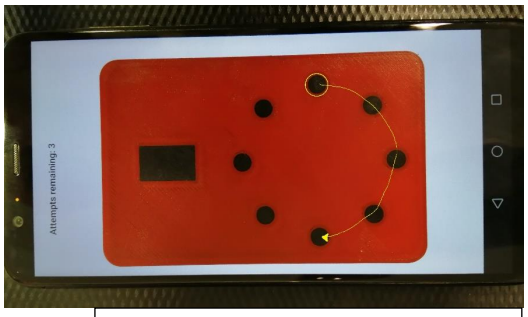


Fig. 1, Starting from the topmost dot, run your finger in a clockwise direction over 4 more dots.

Starting from any of the dots, but for instructional purposes this will show the top-most dot, run your finger over 4 dots in a clockwise direction (Fig 1., starting at the circled dot), then 6 in an anti clockwise direction (Fig. 2, continuing from the circled dot). Finally, ensuring you are not touching any of the other points, tap the rectangle and the authentication is complete (Fig 3.).

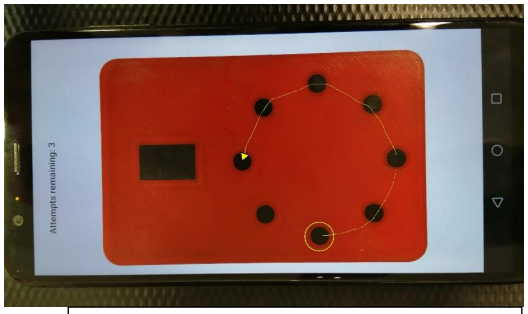


Fig. 2, Keeping your finger on the model, run your finger in an anti-clockwise direction over 6 more dots

Important to note, do not touch the phone screen at any point after starting the authentication, and do not move the object, as the authentication relies on the touch points remaining in the same place on the screen, as such, place the object on the screen initially in such a way that none of it is hanging over the edge.

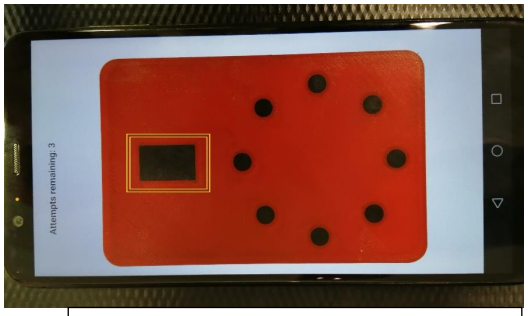


Fig. 3, Finally, release your finger from the final dot touched, and tap the rectangle once.

Figure D.2: *Model instructions issued to participants during the initial meeting to familiarise with assigned model. (part 2/3)*

Pendant

This model is built to act as a pendant that could go on a keychain or necklace. The main idea of this model is to act like a combination lock – turn the layers to the right combination then touch to the screen to unlock your phone.

On the each side of a layer, there will be a number. Align the layers with the numbers 1, 2 and 3 in a column from the top, once the phone is ready, place the object on the phone screen and touch both touch points to authenticate. Do not touch the screen at any point during the authentication, as this will likely make the authentication fail.

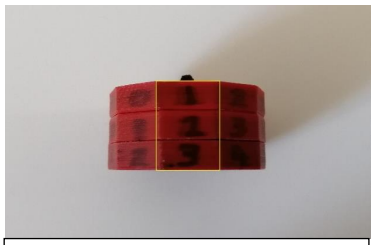


Fig. 1, the layers should be aligned with the numbers 1,2,3 in a column

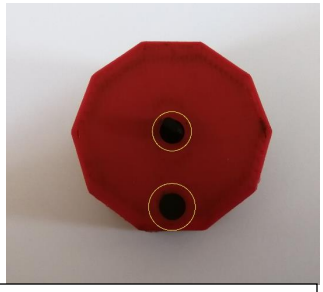


Fig. 2, the two black dots on the top of the pendant should then be touched when the pendant is place on the phone screen

Figure D.3: *Model instructions issued to participants during the initial meeting to familiarise with assigned model. (part 3/3)*

E Initial Interview Survey

In this section, the questions from the survey given in the initial meeting with each participant are specified. For part one, selection questions are specified with the complete list of options given. For part two, these questions all follow the same pattern of selection questions with the choice of one of the following: Completely Disagree, Largely Disagree, Slightly Disagree, Slightly Agree, Largely Agree, Completely Agree.

- Part 1 - Demographics
  - Please enter the ID number you have been assigned. *(Number input)*
  - What is your age? *(Selection, one of: Under 21, 21-25, 26-30, 31-35, 36-40, 41-45, 46-50, Over 50)*
  - Please select your gender: *(Selection, one of: Male, Female, Prefer not to say, Prefer to self-describe).* If 'Prefer to self-describe':
  - Prefer to self describe. *(Open answer)*
  - What is your country of residence? *(Open answer)*
  - Please select your professional status: *(Selection, one of: Student, Employed, Unemployed, Other)*
  - Are you currently working from home? *(Selection, one of: Yes, No)*
  - Are you familiar with other methods of two-factor authentication? *(Selection, one of: Yes, No)*
- Part 2 - ATI Scale
  - I like to occupy myself in greater detail with technical systems.
  - I like testing the functions of new technical systems.
  - I predominantly deal with technical systems because I have to.
  - When I have a new technical system in from of me, I try it out intensively.
  - I enjoy spending time becoming acquainted with a new technical system.
  - It is enough for me that a technical system works; I don't care how or why.
  - I try to understand how a technical system exactly works.
  - It is enough for me to know the basic functions of a technical system.
  - I try to make full use of the capabilities of a technical system.

F Exit Interview Survey

In this section, questions given during the final meeting in the study with each participant are specified. For part one, selection questions are specified with the complete list of options given. For part two, these questions all follow the same pattern of selection questions with a choice of one of the following: Strongly Agree, Agree, Neither Agree nor Disagree, Disagree, Strongly Disagree.

- Part 1 - Model information
  - Please enter the ID number you have been assigned
  - Which model were you tasked with using? *(Selection, one of: Credit Card, Pendant, Cube)*
  - Did the model break or otherwise stop functioning during the study? *(Selection, one of: Yes, No)*
- Part 2 - System usability scale
  - I would like to use this type of authentication frequently
  - Using the model was needlessly complex.
  - Using the model was easy
  - Using the model would require some support from an experienced person
  - The object was well integrated into daily life (ie, it was not jarring to use the object when needed)
  - The object was too inconsistent
  - It would be easy to learn how to use the model for authentication
  - Using the model as authentication was very cumbersome
  - You feel confident you know how to use the model to authenticate
  - There was a lot to learn before you could use the model for authentication

G Exit Interview and Codebook

In this section, the questions given during the exit interview are first specified, with the developed codebook used for the analysis of the meeting transcripts following, along with the number of occurrences for each code.

- Part 1 - Experience in the past week
  - How was interacting with the object in the past week?
    - Was there anything in particular that you like or disliked?
  - Was there anything that went wrong?
  - Was there anything that prevented you from using the item?
  - What do you think of the shape and size of the item?
  - If the item was a commercial product, would you consider buying it?
    - If so, why? If not, why not?
- Part 2 - 2-factor authentication generally
  - Are you familiar with using other 2-factor authentication methods, for example, for your banking or other services?
    - If so, which ones? If not, why?
  - Would you prefer to use this method over other 2-factor authentication methods?
    - If so, why? If not, why not and what could be changed to make it more attractive for use?
  - How secure does it feel to use the provided item for authentication?
    - Is it more, less or about the same as other methods you have used?
  - For which kinds of services would you consider using this type of authentication in your daily life?
    - Why those ones and not others?
  - For which devices would you consider using this type of authentication on?
    - Why those and not others?
- Part 3 - Other models and 3D printing
  - Having had the chance to use all 3 objects, which do you think you would prefer to use?
    - Why? Were there things you liked more about the other objects than the one you were assigned?
  - Would you ever consider owning a 3D printer?

Category	Code	Description	#
Security	familiar_2fa	Participant familiar with two-factor authentication	3
	unsure	Unsure about the security of the models	2
	secure	Feels the models are secure	1
	safe	Feels the models are unlikely to be stolen	2
	shoulder_surfing	Feels vulnerable to shoulder surfing when using the models	1
	requirement	Uses two factor authentication only when required to	2
	no_data	Feels they have nothing important to secure/nothing worth stealing	1
Usability	lacked_feedback	Lacking in feedback when using the models	2
	unique	Unique and novel method of authentication	1
	learning_curve	Felt there was a learning curve to using the models	2
	disliked_handheld_use	Disliked using the models when away from a flat surface	3
	portable	Felt the model was easy to carry around	3
	forgettable	Felt the model was easy to forget to bring	1
	inconsistent	Thought the interaction felt stilted or inconsistent	3
	easy_to_use	Felt the interactions weren't any harder to use than other two factor authentication methods	2
	preferred	Preferred to use the method over other 2FA methods	3
	slide	Models tended to slide on the phone screen	3
	fragile	Models felt fragile	2
	card_favourite	Credit card model was their favourite to use	2
	cube_favourite	Cube model was their favourite	1
	familiar	Familiarity of interaction method was important	2
	enjoy	Enjoyment to use was important	3
	card_liked	Liked interactions with the credit card model	2
	pendant_liked	Liked interactions with the pendant models	2
	cube_likes	Liked interactions with the cube model	3
	future_use	Would consider using in the future	3
Method of use	tabletop_only	Used only on tabletops during the study	2
	banking	Would use for banking and other places 2fa already used for	3
	single_model	Would want to use one model for multiple services	1
	any_device	Would use on any device	2
	stationary_device	Would prefer to use on home computer/laptop only	1
	home_use	Would only use at home	2
	global_use	Would use anywhere	1
3D Printing	would_own	Would consider owning a 3D printer	2
	not_considering	Not currently thinking about owning a 3D printer	1
	no_adoption	Doesn't think there will be widespread adoption of 3D printers	2
	adoption	Thinks there will be widespread adoption of 3D printers	1
	copy_shop	Anticipates 3D printing 'copy shop' types of businesses in the future	2
Commercial	would_not_buy	Would be hesitant to buy any of the models in the future	2
	would_buy	Would buy in the future	1
Improvement	improvement	Suggested improvement	3

Table G.1: *Codebook used for analysis of exit interviews.*

8 Bibliography

F. Aloul, S. Zahidi, and W. El-Hajj. Two factor authentication using mobile phones. In *2009 IEEE/ACS International Conference on Computer Systems and Applications*, pages 641–644, 2009. doi: 10.1109/AICCSA.2009.5069395.

A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon. The phone lock: audio and haptic shoulder-surfing resistant pin entry methods for mobile devices. In *Proceedings of the fifth international conference on Tangible, embedded, and embodied interaction*, pages 197–200, 2010.

J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*, pages 553–567. IEEE, 2012.

V. Braun and V. Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006. doi: 10.1191/1478088706qp063oa.

E. Brockmeyer, I. Poupyrev, and S. Hudson. Papillon: designing curved display surfaces with printed optics. In *Proceedings of the 26th annual ACM symposium on User interface software and technology*, pages 457–462, 2013.

L. Chan, S. Müller, A. Roudaut, and P. Baudisch. Capstones and zebrawidgets: Sensing stacks of building blocks, dials and sliders on capacitive touch screens. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, page 2189–2192, New York, NY, USA, 2012. Association for Computing Machinery. ISBN 9781450310154. doi: 10.1145/2207676.2208371. URL https://doi.org/10.1145/2207676.2208371.

Y. Chen and M. Sinclair. Tangible security for mobile devices. In *Proceedings of the 5th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services*, pages 1–4, 2008.

J. Colnago, S. Devlin, M. Oates, C. Swoopes, L. Bauer, L. Cranor, and N. Christin. "it's not actually that horrible" exploring adoption of two-factor authentication at a university. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–11, 2018.

S. Das, A. Dingman, and L. J. Camp. Why johnny doesn't use two factor a two-phase usability study of the fido u2f security key. In *International Conference on Financial Cryptography and Data Security*, pages 160–179. Springer, 2018.

A. J. DeWitt and J. Kuljis. Aligning usability and security: a usability study of polaris. In *Proceedings of the second symposium on Usable privacy and security*, pages 1–7, 2006.

A. Dmitrienko, C. Liebchen, C. Rossow, and A.-R. Sadeghi. On the (in) security of mobile two-factor authentication. In *International Conference on Financial Cryptography and Data Security*, pages 365–383. Springer, 2014.

T. Fictiv. Recommended wall thickness for 3d printing. https://www.fictiv.com/articles/recommended-wall-thickness-for-3d-printing, 2021. Accessed 2021-11-12.

S. Ghorbani Lyastani, M. Schilling, M. Neumayr, M. Backes, and S. Bugiel. Is fido2 the kingslayer of user authentication? a comparative usability study of fido2 passwordless authentication. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 268–285, 2020. doi: 10.1109/SP40000.2020.00047.

J. Hook, T. Nappey, S. Hodges, P. Wright, and P. Olivier. Making 3d printed objects interactive using wireless accelerometers. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '14, page 1435–1440, New York, NY, USA, 2014. Association for Computing Machinery. ISBN 9781450324748. doi: 10.1145/2559206.2581137. URL https://doi.org/10.1145/2559206.2581137.

Y. Ishiguro and I. Poupyrev. 3d printed interactive speakers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, page 1733–1742, New York, NY, USA, 2014. Association for Computing Machinery. ISBN 9781450324731. doi: 10.1145/2556288.2557046. URL https://doi.org/10.1145/2556288.2557046.

K. Kato and H. Miyashita. 3d printed physical interfaces that can extend touch devices. In *Proceedings of the 29th Annual Symposium on User Interface Software and Technology*, pages 47–49, 2016.

F. Klompmaker, H. Fischer, and H. Jung. Authenticated tangible interaction using rfid and depth-sensing cameras. In *International conference on advances in computer-human interactions*, pages 141–144. Citeseer, 2012.

S. Kratz, T. Westermann, M. Rohs, and G. Essl. Capwidgets: Tangile widgets versus multi-touch controls on mobile devices. In *CHI '11 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '11, page 1351–1356, New York, NY, USA, 2011. Association for Computing Machinery. ISBN 9781450302685. doi: 10.1145/1979742.1979773. URL https://doi.org/10.1145/1979742.1979773.

S. J. Leigh, R. J. Bradley, C. P. Purssell, D. R. Billson, and D. A. Hutchins. A simple, low-cost conductive composite material for 3d printing of electronic sensors. *PloS one*, 7(11):e49365, 2012.

H.-M. C. Leung, C.-W. Fu, and P.-A. Heng. Twistin: Tangible authentication of smart devices via motion co-analysis with a smartwatch. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(2):1–24, 2018.

P. Markert, F. Farke, and M. Dürmuth. View the email to get hacked: Attacking sms-based two-factor authentication. *WAY*, 2019.

K. Marky, M. Schmitz, V. Zimmermann, M. Herbers, K. Kunze, and M. Mühlhäuser. 3d-auth: Two-factor authentication with personalized 3d-printed items. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2020.

K. Marky, K. Ragozin, G. Chernyshov, A. Matviienko, M. Schmitz, M. Mühlhäuser, C. Eghtebas, and K. Kunze. "nah, it's just annoying!" a deep dive into user perceptions of two-factor authentication. *ACM Trans. Comput.-Hum. Interact.*, 2021. ISSN 1073-0516. doi: 10.1145/3503514. URL https://doi.org/10.1145/3503514. Just Accepted.

S. Mayer, X. Xu, and C. Harrison. Super-resolution capacitive touchscreens. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–10, 2021.

M. Ono, B. Shizuki, and J. Tanaka. 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*, UIST '13, page 31–40, New York, NY, USA, 2013. Association for Computing Machinery. ISBN 9781450322683. doi: 10.1145/2501988.2501989. URL https://doi.org/10.1145/2501988.2501989.

H. Peng, J. Mankoff, S. E. Hudson, and J. McCann. A layered fabric 3d printer for soft interactive objects. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 1789–1798, 2015.

J. Prusa. Original prusa i3 mmu2s upgrade kit (for mk2.5s mk3s/+) - org | original prusa 3d printers directly from josef prusa. https://www.prusa3d.com/product/original-prusa-i3-mmu2s-upgrade-kit-for-mk2-5s-mk3s-org/, 2022a. Accessed 2022-03-28.

J. Prusa. Original prusa i3 mk3s+ | original prusa 3d printers directly from josef prusa. https://www.prusa3d.com/category/original-prusa-i3-mk3s/, 2022b. Accessed 2022-03-28.

K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons. A usability study of five two-factor authentication methods. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, pages 357–370, 2019.

M. Sato, I. Poupyrev, and C. Harrison. 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, page 483–492, New York, NY, USA, 2012. Association for Computing Machinery. ISBN 9781450310154. doi: 10.1145/2207676.2207743. URL https://doi.org/10.1145/2207676.2207743.

V. Savage, R. Schmidt, T. Grossman, G. Fitzmaurice, and B. Hartmann. A series of tubes: adding interactivity to 3d prints using internal pipes. In *Proceedings of the 27th annual ACM symposium on User interface software and technology*, pages 3–12, 2014.

M. Schmitz, M. Khalilbeigi, M. Balwierz, R. Lissermann, M. Mühlhäuser, and J. Steimle. 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*, pages 253–258, 2015.

M. Schmitz, J. Steimle, J. Huber, N. Dezfuli, and M. Mühlhäuser. Flexibles: deformation-aware 3d-printed tangibles for capacitive touchscreens. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 1001–1014, 2017.

M. Schmitz, M. Herbers, N. Dezfuli, S. Günther, and M. Mühlhäuser. Off-line sensing: Memorizing interactions in passive 3d-printed objects. In *Proceedings of the 2018 chi conference on human factors in computing systems*, pages 1–8, 2018.

M. Schmitz, F. Müller, M. Mühlhäuser, J. Riemann, and H. V. V. Le. 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*, pages 1–12, 2021.

D. Security. Two-factor authentication methods - tokens passcodes | duo security. https://duo.com/product/trusted-users/two-factor-authentication/authentication-methods/security-tokens, 2019. Accessed 2022-03-28.

M. Sherman, G. Clark, Y. Yang, S. Sugrim, A. Modig, J. Lindqvist, A. Oulasvirta, and T. Roos. User-generated free-form gestures for authentication: Security and memorability. In *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*, pages 176–189, 2014.

E. Stobert and R. Biddle. The password life cycle: User behaviour in managing passwords. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*, SOUPS '14, page 243–255, USA, 2014. USENIX Association. ISBN 9781931971133.

B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor. "i added '!' at the end to make it secure": Observing password creation in the lab. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security*, SOUPS '15, page 123–140, USA, 2015. USENIX Association. ISBN 9781931971249.

K. Willis, E. Brockmeyer, S. Hudson, and I. Poupyrev. Printed optics: 3d printing of embedded optical elements for interactive devices. In *Proceedings of the 25th annual ACM symposium on User interface software and technology*, pages 589–598, 2012.

N.-H. Yu, L.-W. Chan, S. Y. Lau, S.-S. Tsai, I.-C. Hsiao, D.-J. Tsai, F.-I. Hsiao, L.-P. Cheng, M. Chen, P. Huang, et al. Tuic: enabling tangible interaction on capacitive multi-touch displays. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2995–3004, 2011.

V. Zimmermann and N. Gerber. The password is dead, long live the password–a laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies*, 133:26–44, 2020.