First couple slides:

This is the presentation portion of the 4th year computing science individual project. My name is Mark Turner, and I will be presenting tangible 2-factor authentication, a project supervised by Karola Marky. I’ll first be giving some background relevant to the project, then outlining what was done and finally the results obtained.

In recent decades, with the spreading of digital devices, securing one’s data through authentication has become more and more important. While the most common method of authentication, passwords offers a knowledge based security factor and are easy to use in terms of deployment and management, there exists several weaknesses in security such as reused or easy to guess passwords. As a result, 2-factor authentication adds a second factor – usually ownership – to expand on the security of a knowledge based method. However, this also has issues, with many 2fa methods seen as cumbersome due to usability issues, resulting in low adoption rates. Research has been done into many different methods of tangible authentication, and has shown an increased enjoyment level when using such methods, indicating a higher usability level for methods of this type.

T2FA:

This project investigated this combination of tangible 2 factor authentication, hoping to improve on the usability issues of 2fa by making interactions more fun, and potentially opening new avenues of customization.

The method proposed involves the use of 3d printed objects, each of which designed with both a conductive and insulating form of plastic. Interacting with the model activates ‘wires’ of conductive material which, when placed on a capacitive touch screen as implemented in smart phones, can be verified for correctness, as well as activating a unique object ‘footprint’ for verification of ownership.

T2FA and 3D Auth:

This work is a follow up to the research presented in 3D-Auth: Two-Factor Authentication with Personalized 3D-Printed Items. In this paper, different methods of interaction were defined for use in objects of this type, those being Touch, Configuration, Assembly, Arrangement and Augmentation. Prototypes were then built for each of the interaction methods and assessed in a lab study, finding that the method of authentication was generally easy to understand and perform, and indicated a promising usability level. To further investigate this new method of authentication, this study was proposed, with the aims of creating more developed objects and assessing their use in daily life over a period of time.

Online Study:

To begin the creation of more desirable objects, an existing online survey was analysed, looking to find the traits potential end-users wanted to see in these sorts of authentication items. After performing inductive categorization to generalize valid answers, a list of shapes as well as desired sizes was obtained to adapt into working models. \*Talk through the tables briefly\*

Final Models:

With this information, each of the shapes with multiple responses – that is, keyring etc – were given initial designs, with 2 of the ‘too personal’ items being removed from consideration, those being the phone case and the ring wearable, as it was hard to plan for ring size and type of phone participants in the study may have. The initial designs were then given an interaction method from those defined in 3D Auth, excluding augmentation, as this was indicated in the 3D Auth paper to be the least usable method. Rough production drawings were made to plan out sizes and locations of conductive material to facilitate interactions. Another pass was done through the models, removing those using assembly, as this required multiple models and would be cumbersome for users, and the more complicated models, in order to ensure the printed models would be usable very quickly after printing, with no need to remove supports. The remaining 6 models were digitized, another pass through was done removing according to limitations in the app that will be discussed shortly, and one candidate model chosen for each of the 3 remaining interaction methods.

\*At this point be ready to move through the demonstration videos and talk through the models

The first model was the cube, a very popular shape in the survey, this was created to mimic a playing die, with the interaction involving touching different sides of the die to the screen, almost like entering a PIN – the Arrangement method. This covers the knowledge factor, the ownership ‘footprint’ was designed to be the positioning of the pips on the 2 side, but could be implemented on any of the sides, with a more developed version potentially using symbols as with some specialized dice.

The next model was the card, another of the most suggested items, this was created to be similar in dimension to a credit card, so it would easily fit in a wallet or a phone case. The interaction designed for this model involved swiping ones fingers over the circle of black touch points in a similar way to using a safe dial lock, then touching the final ‘enter’ touch point – this was the Touch interaction method. The footprint of the object could be found on the underside of the enter point, in this case implemented as again two conductive dots.

Finally, the last model was the pendant, and while this was lower on the list than the previous two, could be used as a keyring or other hanging object. This took the form of a combination lock, with users to turn each layer of the model until the correct PIN was shown, then place on the screen touching the two black touch points on the top of the model. The footprint in this case was implemented as the position of the outermost dots on the foot of the model, with the central ‘axis’ point used to detect when an attempt is made.

Study App:

To facilitate the assessment of these models, an app had to be created for deployment on participants phones to verify authentications and collect some data through the study period. The app was implemented for Android and was to send notifications at semi-random times of the day, prompting users to authenticate with their model in an attempt to mimic the need for authentication in users’ daily lives. Built in conjunction with the design of the models, it was found that some functions for MotionEvents returned inconsistently through different systems, limiting which functions could be used for verification as participants in the study were to use their own mobile devices. This is what led to a number of the model designs being dropped, like the coin which relied on movement on-screen. The implementation of the app was fairly simple itself, with notification scheduling, authentication checking and data collection, the authentication checking implemented by looking for position and number of touch points active on screen at once.

Study:

Moving on to the study, the purposes of which were to assess the usability of the objects in users’ daily lives, hence a lab study would not be sufficient here. A total of 3 participants signed up for the study, with only one participant for each item. Each participant was asked to be present for an in person meeting, where they would fill out a consent form and demographics survey, as well as be assigned a model for use. They each went away for 1 week and were asked to perform authentications whenever a notification was sent to them, then return for an exit meeting, again with a survey to fill out, data collection from the application, and an exit interview which was later transcribed.

Results:

The study’s results were analysed for qualitative and quantitative data –

The quantitative indicated that the models were quick to use, with authentication attempts improving over time as the participants became more used to their items. This resulted in each of the models taking on average less than 10 seconds to attempt authentications. However, success rate indicated a large number of attempts were required to successfully authenticate, with the lowest at only 15% over all attempts. While this appears to be very worrying, it was found that this was the result of a flawed authentication mechanism, due to the capacitive resolution of touchscreens being slightly different, separate touch points were registered as one in some cases, this was noted in the qualitative results too. Finally, the users completed a System Usability Scale survey which gave an average rating of 57.5, a fairly low score, however also affected by the inconsistent read problem discusses prior.

The qualitative data obtained was gathered by thematic analysis of interview transcripts. Users with a higher affinity for technology noted that they felt the objects weren’t completely secure, with one noting that they felt this way due to their own perception of security being difficult to use, where this method felt more fun, like a toy. The users also leaned more towards using the items when at a desk or flat surface, preferring to use in a more stationary setting for services used rarely. One even suggested that rather than mobile devices, this method would be more appropriate for home computers. Despite this, all of the participants found that the models were easy to carry with them and felt for the most part they were sturdy enough to not break. An issue brough up frequently during the interviews was that of the material, with hard plastic on glass screens, the participants found the models sliding easily, making it harder to use. Overall however, each of the participants indicated they enjoyed the interaction methods, and were eager to see and potentially use more developed versions in the future.

Limitations:

Of course, one big limitation of the study performed was the low number of participants. As such, these results should be considered as preliminary indications of what issues may arise and what opinions may form, and a follow-up study should be performed to obtain more data as many issues may not have been discovered in this study. As well, the flawed study app will have affected some opinions of the participants and certainly the quantitative data obtained, and must be carefully implemented.

The future:

Future research in this area should consider these results – perhaps a focus on portability may not be the best avenue of development for this method of authentication as users have indicated a preference for stationary devices. With the issue with the study app found in this project, raw capacitive data may be more useful and consistent in authentication reading, as well as opening the possibility for more complex models, able to read patterns as demonstrated by Martin Schmitz

If research continues in this area, and these problems are solved, these models could see widespread use, with highly customizable objects capable of being created.

Conclusion:

This study on Tangible 2 Factor Authentication has found the method to be quite promising with preliminary results of a study involving newly created objects showing participants were willing to adopt this method as a new 2fa option, but more research should be done before a final implementation is ready – some issues were unearthed here, however in itself the study was very limited by a low number of participants. With care and further research, this could well become a widely adopted and potentially easily deployable (depending on 3d printing advancements) tool in the future.

Thanks:

Thank you for your time