Usability of Single- and Multi-factor Authentication Methods on Tabletops: A Comparative Study

Anders Bruun, Kenneth Jensen, Dianna Kristensen

Usability of Single- and Multi-factor Authentication Methods on Tabletops: A Comparative Study

Anders Bruun[1], Kenneth Jensen[1,2] and Dianna Kristensen[1,3]

[1]Aalborg University, Selma Lagerlöfs Vej 300
DK-9220 Aalborg Oest
bruun@cs.aau.dk
[2]Analytech, Bøgildsmindevej 21
DK-9400 Nørresundby
keje89@gmail.com
[3]DanDomain, Normansvej 1
DK-8920 Randers NV
dhk@dandomain.dk

Abstract. With the introduction and adoption of tabletop technologies a need for different user authentication mechanisms has arisen. Tabletops support close collaboration between users, typically in close physical proximity and such settings are more vulnerable to shoulder surfing attacks compared to desktops settings where users are more distantly located. Previous studies on desktop interfaces have shown that multi factor authentication provides a higher level of security than single factor authentication. This study extends previous work by comparing the usability of several authentication methods applied in tabletop settings. The aim of the study is to contribute with proposals on which authentication methods to apply when engineering user interfaces for tabletop devices. We compare single factor and multi-factor authentication mechanisms from a usability perspective.

Keywords: Usability, tabletop, multi-factor, authentication, TUI.

1 Introduction

Tabletop technologies are applicable in public and private spaces where large interfaces foster collaboration between users interacting with digital information [8]. Although promising, we also find new security shortcomings within tabletop settings as the nature of these devices is for co-located collaboration. One such shortcoming is that of shoulder surfing attacks, which is when a person makes malicious observations to obtain e.g. write access in personal documents belonging to one of the collaborators. In the case of collaborative settings with tabletops the authentication information is relatively easy compromised as everyone around the tabletop can see what every-

adfa, p. 1, 2011.

one else does [8]. Another security threat is smudge attacks, which is when fingerprint oil is left on a display when using direct touch to interact. Such oil traces can be used to deduce authentication credentials [1]. Thus, close physical proximity in collaborative settings decrease the level of security.

In conventional desktop settings several authentication methods have been proposed for validating users and to grant permission to access personal data. A common knowledge-based authentication approach is the username/password combination. Literature reports of three authentication factors: K*nowledge factor* (information you know), *possession factor* (physical object you possess) and the *inheritance factor* (biometric properties you possess) [7, 10].

The growing risk of compromising passwords and usernames (not only in tabletop settings) has led to alternative methods accommodating a higher level of security. One such method is multi-factor authentication which is considered stronger than single factor authentication [2, 10]. Multi-factor authentication combines two or more of the above authentication factors e.g. a password (knowledge factor) and a keycard (possession factor) for authentication.

Currently, only a few studies concern security aspects of tabletop technologies [8]. Also, the focus in authentication research has primarily been on security aspects and lesser on usability aspects. Examples of studies emphasizing security over usability are [8, 10, 11]. Design of security systems often conflicts with usability concerns, although the two aspects are important to address [2, 4]. Gutmann and Grigg [4] for instance state that users ignore secure systems and choose those that are more usable, i.e. usability is prioritized over security. Thus, the aim of the study presented in this paper is to compare different single- and multi-factor authentication methods with respect to usability concerns.

2 Related Work

In this section, we present related work within single and multi-factor authentication methods in relation to desktop and tabletop technologies. Recent research has been on multi-factor authentication methods [5, 8, 10] on various systems.

Braz et al. [2] presents a comparative study of authentication methods applied on traditional desktop applications in which they compare existing methods such as password, proximity card, multifunction card, public key, fingerprint etc. They compare authentication methods on the parameters of advantages and disadvantages in relation to security, usability and input time. Findings of that study indicate that the highest level of security can be found in the three methods of voice (inheritance), password and PIN (knowledge). The three systems with the highest level of usability are: Password, PIN and retina/iris scanning. They conclude that there is a need for more focus on usability to make reliable, effective and usable authentication systems [2].

Kim et al. [8] specify methods for one-factor authentication on tabletops. The aim was to reduce the risk of shoulder surfing. That study was based on one user logging into the system and two observers that afterwards tried to login as that user, hereby

simulating a shoulder surfing attack. Findings in that study are based on measures of task completion times and number of successful shoulder surfing attacks.

Marquardt et al. [9] specify a system using a fiduciary-tagged glove. Fiduciary-tags are like barcodes and QR codes. By placing 15 tags strategically on the glove to identify which part of the hand is actually touching the surface their system enhanced gesture recognition and thereby expanded the interaction possibilities. The glove also makes it possible to identify a specific user, as the glove is meant to be a unique possession [9]. In terms of related work we did not find any studies comparing single and multi-factor authentication methods on tabletop technologies.

3 Method

In this study the two independent variables are: One-factor and two-factor authentication methods. These two variables have been chosen based on the popularity in modern systems and because they will likely require different completion times. We set up four authentication conditions: Three based on single-factor and one on multi-factor. The four conditions were evaluated by measuring task completion times and the System Usability Scale (SUS) [3].

Throughout the study we applied Microsoft Surface 2.0 as the tabletop device. We chose to create a similar layout of all developed prototype designs in order to avoid experimental bias related to differences in designs.

3.1 One-Factor Authentication

We designed and developed three prototypes for one-factor authentication. Two of these focus on the knowledge factor through the use of a username/password combination and a username/PIN combination. The third condition focuses on the possession factor by using a Tangible User Interface (TUI).

We evaluated knowledge factor authentication through the use of PIN and Password as Braz et al. [2] found these to have the highest level of security and usability in desktop settings. In collaborative settings around a tabletop it is not enough to settle for just a PIN or a password as is the case on e.g. a laptop or a mobile phone where the devices are personal. As the tabletop is shared among multiple users, the individual person needs to be identified as anyone around the tabletop could enter a PIN/password. To accommodate this situation we added the established knowledge factor of username hereby keeping the conditions in a single-factor mode.

Authentication based on possession is evaluated through the use of a TUI based on fiduciary tags, which Marquardt et al. [9] found to be a feasible authentication method.

Username and PIN Condition (UsPi). In the UsPi condition participants applied a combination of a username and PIN for authentication. User input was made through an onscreen QWERTY keyboard and a numpad was provided for entering the PIN. See Fig. 1 for an example.

Username and Password Condition (UsPa). In the UsPa condition the user uses a combination of a username and password. The purpose is to use this condition as a benchmark for the four other conditions, as this is a common authentication method applied in traditional desktop settings.

Tag. In the tag condition the participants applied a TUI. The TUI is implemented using a fiduciary tag, which is a paper-based 8 bit picture code that Microsoft Pixelsense recognizes. With the Tag condition the user just places the TUI on the tabletop in order to authenticate.

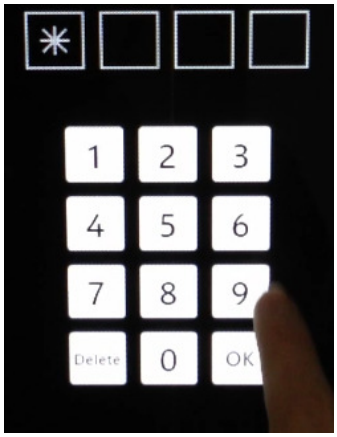

Fig. 1. UsPi prototype, knowledge factor authentication

3.2 Two-Factor Authentication

The second variable is two-factor authentication, where we designed and developed one prototype focusing on a combination of using a TUI and PIN.

Tag and PIN condition (TaPi). The TaPi condition uses a TUI with a PIN input. The process to authenticate is first to place the TUI. When the TUI is registered by the tabletop, a numpad appears relative to the TUI. The user then enters a four digit PIN and presses OK.

3.3 Participants

Each system was evaluated by university students. The experiment had 16 participants of which two were female. Participant's mean age was 24 (SD=3.66). They had one to eight years of experience using touch devices, such as tablets and smartphones. Only two had previous experience using tabletops. Participants were familiar with single- and multi-factor authentication methods on conventional desktop and laptop PCs.

3.4 Procedure

The study was conducted within a lab facility at the university and the room was darkened to limit interference of sunlight on the tabletop. The experiment was conducted as a within-subject study, i.e. each condition had 16 participants. To reduce ordering bias the usage of prototypes was randomized.

The procedure of the experiment was as follows: 1) Participants filled the demographic questionnaire, 2) Participants were informed of the purpose and procedure, 3) Credentials for authorization (in written form) was given to the participants, 4) Participants tried to authorize themselves using the credentials, 5) After successful (or unsuccessful) attempts for each prototype, participants filled in the SUS questionnaire, 6) Repeat steps 4 and 5 until participants completed all four conditions and 7) Participants were interviewed to elaborate on their opinion on the different prototypes.

3.5 Data Analysis

The data analysis was conducted by the two last authors of this paper who analyzed all data. For each participant we collected four videos, four SUS questionnaires and one interview of five to 15 minutes. In total we collected 64 videos, 64 SUS questionnaires and 16 interviews. Each video was analyzed and usability problems were noted. Afterwards the two last authors made a comparison of the identified problems. To validate the qualitative video analysis the agreement between the evaluators was calculated based on the measure of any-two agreement. In this study the two authors agreed on 22 of the 44 identified problems, i.e. an any-two agreement of 50%. The any-two agreement for this study is at the higher end compared to the agreement of 6% to 45% mentioned in [6].

4 Results

In this section we present our findings. First, the SUS scores are presented. Secondly task completion time results are presented followed by qualitative results from the interviews and video analysis of usability problems.

4.1 System Usability Scale

Table 1 provides a summary of the average SUS scores given for each of the four prototypes. This shows that the UsPi prototype scores lowest with an average of 68.75 (SD=19.3) while the TaPi and Tag prototypes scores highest with 92.5 (SD=9.9) and 90.2 (SD=7.5) respectively.

	UsPi	UsPa	TaPi	Tag
Avg (SD)	68.75 (19.3)	84.1 (13)	92.5 (9.9)	90.2 (7.5)

Table 1. SUS scores for each of the prototypes and user.

A one-way ANOVA test shows significant differences between one or more of the conditions (df-resid=60, F=10.56, $p<0.001$). A Tukey's pair-wise comparison test reveals significant differences between the UsPi prototype and all other prototypes ($0.001<p<0.01$). There are no significant differences between the UsPa, TaPi and Tag prototypes ($p>0.1$). Thus, the UsPi protype receive significantly lower SUS scores than all other prototypes.

4.2 Task Completion Times

Table 2 shows an overview of the task completion times for all participants. The slowest condition on average is the UsPi prototype with a mean of 34.4 (SD=28.8) seconds while the fastest is the Tag prototype with 3.6 (SD=0.8) seconds.

	UsPi	UsPa	TaPi	Tag
Avg (SD)	34.4 (28.8)	29.2 (16.9)	10.4 (3)	3.6 (0.8)

Table 2. The Completion time in seconds for each prototype and user.

A one-way ANOVA test on the task completion times show significant differences between one or more of the prototypes (df-resid=60, F=12.32, $p<0.001$). A Tukey's Pair-wise comparison test reveals significant differences between the UsPi/UsPa prototypes compared to the TaPi/Tag prototypes ($p<0.001$). Completion times between the UsPi and UsPa prototypes are not significant ($p>0.1$). Also, we found no significant differences between the TaPi and Tag prototypes ($p>0.1$). Thus, the UsPi and UsPa prototypes have significantly longer completion times than the TaPi and Tag prototypes.

4.3 Qualitative Data

We gathered two types of qualitative data in our study. The first were the results of the preference questions asked in the post test interview, the second were the usability issues extracted from videos. The most severe usability problems are presented here and all relate to platform and implementation issues.

We identified a tag-flickering problem in the prototypes based on a TUI (TaPi and Tag). The TUI began to sporadically flick causing the tabletop device to lose track of the TUI. Participants also mentioned confusion in the interpretation of how to use the progress bar in case of the UsPi prototype. A participant mentioned: *"I was confused on how to continue and tried to press the keyboard and the progress bar [while pointing at the four spaces in the UsPi prototype]"*. One participant also experienced problems with the keyboard in the UsPi prototype: *"I searched for the Tab button but could not find it at all, and then I was in trouble of how I should continue from here"*.

5 Discussion

In relation to task completion time, the possession-based TUI prototypes were significantly faster than the knowledge based. As expected, the single-factor Tag prototype was faster than the multi-factor TaPi prototype. Although faster, the Tag prototype received lower SUS ratings compared to the TaPi prototype. This indicates that task completion time is not corresponding entirely to the satisfaction ratings provided in the SUS scores. This is also supported by the finding of the UsPa prototype having significantly longer task completion time, yet similar SUS ratings compared to the TaPi and Tag prototypes. When asked which of the prototypes participants preferred, most mentioned TaPi followed by Tag. Thus, although the Tag prototype resulted in faster completion times it was not the preferred authentication method. An explanation for this observation is related to security concerns. We asked participants if the type of personal information accessed would affect their choice of authentication method. Several mentioned that they wanted to use TaPi for authenticating access to personal information while some also mentioned that they would apply a TUI for less critical information access. This indicates that participants were willing to use an authentication method that takes more time to complete in order to increase security in collaborative settings, i.e. they felt less secure using single-factor authentication based on possession only. Furthermore, some of the participants stated a concern towards the ease of replicating the particular fiduciary tag applied in our case. A consequence of the ease to replicate it is that malicious people can easily create another tag and hereby a false identity. So, in general the tag alone is not perceived to be secure enough for participants. The preference of the Tag and PIN combination could also be attributed to the novelty of this type of user interface, which could make it more interesting for first time users compared to the well-known Username/Password combination. UsPi performed worst in terms of SUS ratings and task completion times. This is likely because the username and PIN combination is rarely used elsewhere, which is also reflected in some of the severe usability problems identified. In terms of related work, both TUI prototypes had average completion times in same range as those identified by Braz et al. [2] in desktop settings. However, findings in [2] and our study cannot be compared directly as desktops and tabletops are two very different technologies with varying interaction patterns. Nevertheless it shows that similar task completion times can be obtained in tabletop settings.

In sum, the fastest of our authentication methods was the Tag and second fastest was TaPi, both having average completion times in same range as in related work dealing with desktop settings. The condition which had the highest level of usability was TaPi while the second highest score was attributed to the Tag prototype. In contrast, the widely used single-factor method of username and password received a slightly lower SUS score and it had significantly longer completion times.

6 Conclusion

The aim of the study was to contribute with proposals on which authentication methods to apply when engineering tabletop devices and user interfaces. We have empha-

sized a usability perspective in a comparison of single-factor and multi-factor authentication methods. We found that the combination of a TUI and PIN (TaPi) provided the highest level of usability. However, TaPi was not the fastest authentication method, but participants perceived TaPi authentication to be the most secure. Surprisingly, the well-established single factor authentication method based on username and password was not preferred. These are key points to consider when engineering user interfaces for tabletop technologies.

Authentication is typically conducted several times during a day. For this reason it would also be relevant to extend our work with longitudinal studies of usability, i.e. the usability of first time usage is only a subcomponent in the evaluation of authentication methods for tabletops.

7 References

1. Aviv, A.J., Gibson, K., Mossop, E., Blaze, M. and Smith, J.M. Smudge attacks on smartphone touch screens. In *Proc.* WOOT. USENIX Association (2010).
2. Braz, C. and Jean-Marc, R. Security and usability: the case of the user authentication methods. In Proc. IHM. ACM (2006).
3. Brooke, J. SUS-A quick and dirty usability scale. In P. W. Jordan, B. Thomas, B. A. Weerdmeester, & A. L. McClellan (eds) Usability Evaluation in Industry. Taylor and Francis (1996).
4. Gutmann, P. and Grigg, I. Security Usability.Security & Privacy 3, 4, pp.56-58. IEEE (2005).
5. Harini, N. and T. R. Padmanabhan. 2CAuth: A New Two Factor Authentication Scheme Using QR-Code. International Journal of Engineering and Technology (2013).
6. Hertzum, M. and Jacobsen, N.E. The evaluator effect: A chilling fact about usability evaluation methods. International Journal of Human-Computer Interaction 13, 4, pp. 421-443.
7. Jin, A.T.B, Ling, D.N.C. and Goh, A. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern recognition 37, 11, pp. 2245-2255. Elsevier (2004).
8. Kim, D., Dunphy, P., Briggs, P., Hook, J., Nicholson, J.W., Nicholson, J. and Olivier, P. Multi-touch authentication on tabletops. In Proc. CHI. ACM (2010).
9. Marquardt, N., Kiemer, J. and Greenberg, S. What caused that touch?: expressive interaction with a surface through fiduciary-tagged gloves. In Proc. ITS. ACM (2010).
10. Sabzevar, A.P. and Stavrou, A. Universal Multi-Factor Authentication Using Graphical Passwords. In Proc. SITIS. IEEE (2008).
11. Qin, Y., Yu,C., Jiang, H., Wu, C. and Shi, Y. pPen: enabling authenticated pen and touch interaction on tabletop surfaces. In Proc. ITS. ACM (2010).