
There may be differences between this version and the published version. You are advised to consult the publisher’s version if you wish to cite from it.

© The Authors 2016. This is the author's version of the work. It is posted here for your personal use. Not for redistribution. The definitive Version of Record was published in the Proceedings of the 34th Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems, San Jose, CA, USA, 07-12 May 2016, pp. 2156-2164. ISBN 9781450340823
https://doi.org/10.1145/2851581.2892314.

http://eprints.gla.ac.uk/170228/

Deposited on: 5 October 2018
GazeTouchPass: Multimodal Authentication Using Gaze and Touch on Mobile Devices

Mohamed Khamis\textsuperscript{1}, Florian Alt\textsuperscript{1}, Mariam Hassib\textsuperscript{1,2}, Emanuel von Zezschwitz\textsuperscript{1}, Regina Hasholzner\textsuperscript{1}, Andreas Bulling\textsuperscript{3}

\textsuperscript{1} Media Informatics Group, University of Munich (LMU), Munich, Germany
{mohamed.khamis, florian.alt, mariam.hassib, emanuel.von.zezschwitz}@ifi.lmu.de, hasholzner@cip.ifi.lmu.de

\textsuperscript{2} VIS, University of Stuttgart, Stuttgart, Germany
mariam.hassib@vis.uni-stuttgart.de

\textsuperscript{3} Perceptual User Interfaces Group, Max Planck Institute for Informatics, Saarbrücken, Germany
bulling@mpi-inf.mpg.de

Abstract
We propose a multimodal scheme, GazeTouchPass, that combines gaze and touch for shoulder-surfing resistant user authentication on mobile devices. GazeTouchPass allows passwords with multiple switches between input modalities during authentication. This requires attackers to simultaneously observe the device screen and the user’s eyes to find the password. We evaluate the security and usability of GazeTouchPass in two user studies. Our findings show that GazeTouchPass is usable and significantly more secure than single-modal authentication against basic and even advanced shoulder-surfing attacks.

Author Keywords
Multimodal Authentication; Gaze Gestures; Mobile Devices

ACM Classification Keywords
H.5.2 [Information Interfaces and Presentation]: User Interfaces; K.6.5 [Computing Milieux: Security and Protection]: Authentication

Introduction
With mobile devices enabling ubiquitous access to sensitive information, there is a need to protect access to such devices. Meanwhile, authentication schemes are prone to shoulder-surfing attacks [20], where a bystander observes a user while authenticating. The attacker then gets hold of the device and tries to authenticate and access sensitive data.
Recent work proposed schemes that are more resistant to observations [11, 25]. However in most cases, attacking state of the art schemes involves observing only one entity – the phone – in preparation for an attack.

At the same time high-resolution front-facing cameras made it possible to track users’ gaze on mobile devices [12, 13, 14, 21, 27]. These advances took gaze-based authentication from desktop systems [4, 5, 16], to mobile devices [17]. This work combines gaze and touch input for secure user authentication on off-the-shelf mobile devices.

We propose a novel multimodal scheme, GazeTouchPass, that makes mobile user authentication more robust against shoulder-surfing by requiring attackers to simultaneously observe both the user’s eyes and the phone (Figure 1). GazeTouchPass combines gaze and touch input into multimodal passwords (e.g. left-3-right-4).

The contributions of this work are two-fold. First, we introduce the concept and the implementation of GazeTouchPass, a novel multimodal authentication scheme that secures mobile devices against classic and even advanced shoulder-surfing attacks. Second, we report on an evaluation of the system’s usability and security, and compare it to state-of-the-art schemes. Our findings show that multimodal authentication using gaze and touch is significantly more secure than single-modal authentication against basic and even advanced shoulder-surfing attacks.

**Threat Models**

GazeTouchPass addresses two threat models, in both models the user is in a public space that is not under the control of the attacker. The attacker is familiar with the system and knows how to provide a password.

**Iterative attacks.** The attacker can observe the user several times (e.g. a colleague at work) from different viewpoints. The attacker exclusively focuses on one modality per observation – on the users’ eyes (eyes-view) and then on the input on the screen (phone-view), or vice versa. The challenges of this attack are to (a) correctly remember both sequences and to (b) correctly combine them later.

**Side attacks.** The attacker observes the user while authenticating once (e.g. in a subway) from an angle that allows the user’s eyes as well as the user’s input on the touchscreen to be observed. The distance between the attacker and the user is close enough to see the touchscreen, but far enough to reduce the effort of switching focus back and forth between the user’s eyes and the device’s display.

**GazeTouchPass: Multimodal Passwords**

Based on these threat models we propose GazeTouchPass, a multimodal authentication scheme in which users define four symbols, each can be entered either via touch (a digit between 0 and 9) or via gaze (gazing to the left and to the right). Consecutive gaze inputs to the same direction would then need to be separated by a gaze to the front.

We expect that the more switches between input modalities are used within a single password, the more difficult it will be to observe it. For example, we expect: “1-left-2-right” (3-switches) to be more secure than “1-2-left-right” (1-switch). As for side attacks, each switch in input modality is equivalent to a switch of the attacker’s focus between the touchscreen and the eyes. In case of iterative attacks, as switches between modalities increase, so do the possible combinations of observations from the eyes-view and the phone-view. Examples of passwords with different number of modality switches are shown in Table 1.
The login interface consists of 10 buttons similar to a common 10-digit keypad (see Figure 1). Users log in by touching digits and moving their eyes. The system is implemented as an Android application and does not require any additional hardware. The user’s face and eyes are first detected using the Viola-Jones detector [24] through the device’s front-facing camera. On top we then use a calibration-free gaze estimation approach similar to a method recently introduced for interaction with public displays [28]. Our method calculates the distance between the center of the face and the pupil for each eye. Discrete gaze directions are then estimated based on the ratio between both distances.

### Usability Study

The aim of this study is to analyze the usability of Gaze-TouchPass and to collect video recordings of gaze and touch input for the subsequent security study. In a repeated measures experiment, each participant performed 16 authentications (4 passwords × 4 conditions) using randomly generated passwords. We recruited 13 participants (9 females), aged between 21 and 35 years ($M = 25.23$, $SD = 3.8$). We logged all login attempts and recorded the participants using three HD video cameras (see Figure 2).

Each participant performed a training run per condition, to get acquainted with the system. These runs were excluded from further analyses. At each authentication attempt, the experimenter read out the password to be entered according to a previously generated, randomized list. Participants repeated entry in case of false login. The study was concluded with a semi-structured interview. We evaluated the system’s usability based on input speed and error rate.

**Input Speed.** We measured the time taken to input the passwords. We excluded 3 out of 72 input time measurements prior to analysis as outliers ($> μ + 3×SD$). No significant main effects were found for number of modality switches on authentication time ($p > 0.05$). Figure 3 suggests that mean authentication times do not vary greatly among different number of modality switches.

**Error Rate.** We also logged the number of failed login attempts, which were either due to incorrect input or false detection by the system. A Pearson chi-square test showed no significant effect of number of modality switches on error rate $χ^2(30) = 33$, $p = 0.32$. Figure 5 shows that there were fewer errors in the case of passwords with 3-switches. While providing multiple consecutive gaze gestures can be error prone, having 3 switches in a 4-digit password can be achieved only by alternating gaze gestures and digits.

### Table 1: Examples of password conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-switches (baseline)</td>
<td>1-2-3-4 left-right-left-left</td>
</tr>
<tr>
<td>1-switch</td>
<td>left-1-2-3 1-2-left-right</td>
</tr>
<tr>
<td>2-switches</td>
<td>left-1-left-right left-1-2-right</td>
</tr>
<tr>
<td>3-switches</td>
<td>1-left-2-right left-1-right-2</td>
</tr>
</tbody>
</table>

Figure 2: The usability study setup. Cameras A and B simulate an iterative attack (observing the phone screen and user’s eyes separately), while Camera C simulates a side attack (observing the phone screen and user’s eyes simultaneously).
Figure 3: Mean authentication times for passwords with different numbers of modality switches. Authentication times do not vary significantly among different number of modality switches. Overall mean authentication time is 3.1 seconds (SD = 1.3).

Qualitative Feedback. Six out of 13 participants reported they would use GazeTouchPass as a primary authentication scheme. Nine reported that they would not use it for daily unlocking, but rather for insecure situations or to protect sensitive data, such as their online banking apps. One participant indicated that she would be willing to use GazeTouchPass for a one-time unlock (e.g. when switching the phone on). Four participants said they would not be willing to do anything extra for higher security; two of them added that they do not use any lock mechanism on their phones.

Figure 4: (a) A participant observing the side-view during a side attack. (b) A participant observing the eyes-view as part of an iterative attack. (c) When performing iterative attacks, participants noted the pauses between gaze gestures then tried to fill the gaps with digits observed through the phone-view.

Security Study
In the security study, we used the videos recorded from the preceding study to evaluate the security of GazeTouchPass. Following a repeated measures design, participants attacked passwords with all four possible number of switches and observed from all views using the videos recorded during the usability study. Every participant attacked 8 passwords of each condition of $n$-switches – half of which were side attacks (side-view), while the others were iterative attacks (phone-view and eyes-view) where the experimenter alternated the order of the observed view. Each participant attacked 32 passwords. The order of videos was randomized per participant. To avoid learning effects, no participant attacked the same password from different views.

We recruited 13 participants (6 females), aged between 21 and 33 years ($M = 24.2$, $SD = 3.4$), through mailing lists, none of whom had participated in the usability study. Participants were compensated with a 10 Euro voucher. In addition, all participants took part in a draw for an additional 20 Euro voucher, where chances of winning increased with the number of successfully attacked passwords.

The experimenter introduced the study procedure, the task, and the rewarding mechanism. After explaining the system, participants had the chance to try and get acquainted with the app themselves. They were given draft papers, then the experimenter started playing the videos. Based on their observations, participants provided up to three guesses (Figure 6). The study was concluded with a questionnaire and a semi-structured interview. In total, participants performed $13 \times 32 = 416$ attacks with up to three guesses each.
Successful Attacks. For every attack we calculated the Levenshtein distance between the guesses and the correct password. Only the guess closest to the correct password was considered for further analysis. Moreover, we calculated the overall success rate in attacking passwords for each number of modality switches and for each attack type (iterative attack vs side attack). An attack is successful if at least one guess matched the correct password. Figure 6 summarizes the successful attack rate against passwords with different number of modality switches, observed through the side-view or through the phone-view and the eyes-view.

A repeated measures ANOVA showed significant main effects for number of modality switches on attack success ($F_{3,36} = 3.86, p < 0.05$). This suggests that distance between the guesses and the correct password depends on the modality switches. Post-hoc analysis using Bonferroni correction showed a significant difference ($p < 0.05$) in attack success for passwords with 0-switches ($M = 1.25, SD = 0.14$) compared to those with 3-switches ($M = 1.9$).

There were significant main effects for the view angle on attack success ($F_{1,12} = 51.05, p < 0.0001$). No interaction effects were found between the number of modality switches and the view angle ($p > 0.05$). Post-hoc analysis using Bonferroni correction revealed that there was a significant difference ($p < 0.0001$) in attack success for passwords attacked iteratively ($M = 1.38, SD = 0.138$) compared to passwords attacked from the side ($M = 1.913, SD = 0.123$). This suggests that guesses against passwords observed iteratively are closer to the correct password compared to those observed from the side.

**Successful Attacks.** For every attack we calculated the Levenshtein distance between the guesses and the correct password. Only the guess closest to the correct password was considered for further analysis. Moreover, we calculated the overall success rate in attacking passwords for each number of modality switches and for each attack type (iterative attack vs side attack). An attack is successful if at least one guess matched the correct password. Figure 6 summarizes the successful attack rate against passwords with different number of modality switches, observed through the side-view or through the phone-view and the eyes-view.

A repeated measures ANOVA showed significant main effects for number of modality switches on attack success ($F_{3,36} = 3.86, p < 0.05$). This suggests that distance between the guesses and the correct password depends on the modality switches. Post-hoc analysis using Bonferroni correction showed a significant difference ($p < 0.05$) in attack success for passwords with 0-switches ($M = 1.25, SD = 0.14$) compared to those with 3-switches ($M = 1.9$).

Successful Attacks. For every attack we calculated the Levenshtein distance between the guesses and the correct password. Only the guess closest to the correct password was considered for further analysis. Moreover, we calculated the overall success rate in attacking passwords for each number of modality switches and for each attack type (iterative attack vs side attack). An attack is successful if at least one guess matched the correct password. Figure 6 summarizes the successful attack rate against passwords with different number of modality switches, observed through the side-view or through the phone-view and the eyes-view.

A repeated measures ANOVA showed significant main effects for number of modality switches on attack success ($F_{3,36} = 3.86, p < 0.05$). This suggests that distance between the guesses and the correct password depends on the modality switches. Post-hoc analysis using Bonferroni correction showed a significant difference ($p < 0.05$) in attack success for passwords with 0-switches ($M = 1.25, SD = 0.14$) compared to those with 3-switches ($M = 1.9$).

Table 2: Authentication times using GazeTouchPass compared to state-of-the-art schemes that use gaze-based authentication [6, 8, 10, 16, 17], input-splitting (e.g. XSide [7]) and multiple modalities [1, 2, 3].
Discussion
GazeTouchPass is particularly secure against side attacks (only 15%-21% success rate). Iterative attacks are complicated but possible in optimal conditions (23%-46%), given that the adversary paid attention to all inputs and noted the gaps between them (see Figure 4c). It should be noted that we assume the attacker knows how the observed system works. The proposed threat models are realistic yet ensure optimal conditions. Nevertheless, GazeTouchPass is more secure than most comparable systems (see Table 3).

Mean authentication time using GazeTouchPass is approximately 3.1 seconds. While this is slower than less secure schemes (von Zezschwitz et al. [26] report 1.5 seconds for PINs and 3.13 seconds for patterns), GazeTouchPass is faster than security-optimized state-of-the-art authentication systems (see Table 2). Overall, and as several participants indicated, GazeTouchPass can be particularly useful as a secondary authentication mechanism that users can choose to opt to when feeling observed (e.g. public setting) or when accessing critical data (e.g. online banking).

GazeTouchPass achieves a balance between security and usability, with low authentication times and high observation resistance. Tables 2 and 3 show that it is faster and more secure than gaze-based schemes [6, 8, 10, 16]. Comparing GazeTouchPass to mobile-based schemes that use multiple modalities, we found that although the security of PhoneLock [1], SpinLock [2], TimeLock [3], ColorLock [3] and the system by Liu et al. [17] was not evaluated in a way comparable to our studies, our system requires shorter login times (see Table 2), and uses a higher password space (12^n) than that of [17]. XSide [7] splits the input using a double-sided touchscreen. Still GazeTouchPass is faster and can work on off-the-shelf mobile devices without additional hardware. Similarly, the number of switches in an XSide password influences its security; in most cases GazeTouchPass is more resistant to observations (see Table 3).

Limitations and Future Work
While GazeTouchPass shows that multimodal passwords are significantly more secure than single-modal ones, iterative attacks are still possible and perceived to be relatively easy to perform. Future work should focus on increasing resistance to iterative attacks while maintaining usability. One possible approach is to introduce a random cue [19] to the user that would complicate attempts to combine observations from multiple views. We will also study the memorability and practical password space of GazeTouchPass.

Video-based eye tracking has its known limitations; varying light conditions, reflections of eye glasses and heavy makeup can affect the quality of eye tracking [18]. For this reason we opted for simple eye gestures that can be robustly detected by frontal-cameras. However, the use of better eye tracking equipment (e.g. infrared light sources and sensors) can enable a wider range of eye movements to be detected robustly. Future systems can use different types of eye movements. For example, the smooth pursuits eye movement has recently gained attention in enabling calibration-free gaze-based interaction [5, 9, 15, 22, 23].

Conclusion
In this paper we introduced multimodal authentication combining gaze and touch on mobile devices. GazeTouchPass is significantly more secure than single modal systems, particularly against side attacks due to having to quickly switch focus between phone and eyes. Its usability compares favourably to state-of-the-art schemes. Our conclusion is that the use of multiple modalities can greatly enhance the security of authentication systems against advanced as well as basic threat models, while maintaining high usability.

<table>
<thead>
<tr>
<th>System</th>
<th>Successful attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>GazeTouchPass</td>
<td></td>
</tr>
<tr>
<td>3-switches (Side)</td>
<td>15%</td>
</tr>
<tr>
<td>3-switches (Iterative)</td>
<td>23%</td>
</tr>
<tr>
<td>2-switches (Side)</td>
<td>15%</td>
</tr>
<tr>
<td>2-switches (Iterative)</td>
<td>37%</td>
</tr>
<tr>
<td>1-switches (Side)</td>
<td>21%</td>
</tr>
<tr>
<td>1-switches (Iterative)</td>
<td>46%</td>
</tr>
<tr>
<td>0-switches (Side)</td>
<td>25%</td>
</tr>
<tr>
<td>0-switches (Iterative)</td>
<td>63%</td>
</tr>
<tr>
<td>EyePassShapes [6]</td>
<td>42%</td>
</tr>
<tr>
<td>EyePIN [8]</td>
<td>55%</td>
</tr>
<tr>
<td>XSide [7]</td>
<td></td>
</tr>
<tr>
<td>front 1-switch start</td>
<td>38%</td>
</tr>
<tr>
<td>front 1-switch end</td>
<td>13%</td>
</tr>
<tr>
<td>front 2-switches</td>
<td>28%</td>
</tr>
<tr>
<td>back 1-switch start</td>
<td>19%</td>
</tr>
<tr>
<td>back 1-switch end</td>
<td>16%</td>
</tr>
<tr>
<td>back 2-switches</td>
<td>9%</td>
</tr>
</tbody>
</table>

Table 3: Successful attack rates using GazeTouchPass compared to state-of-the-art schemes that use gaze-based authentication [6, 8] and input-splitting (e.g. XSide [7]).

Some relevant systems were excluded from this table as their security was not evaluated in a way comparable to our studies [1, 2, 3, 10, 16, 17].
References


