# GlassPass: Tapping Gestures to Unlock Smart Glasses

MD. Rasel Islam
Department of Human Factors Engineering, UNIST
Ulsan, Republic of Korea
rasel@unist.ac.kr

Doyoung Lee
Department of Human Factors Engineering, UNIST
Ulsan, Republic of Korea
dylee.issac@gmail.com

Liza Suraiya Jahan
Department of Human Factors Engineering, UNIST
Ulsan, Republic of Korea
liza@unist.ac.kr

Ian Oakley
Department of Human Factors Engineering, UNIST
Ulsan, Republic of Korea
ian.r.oakley@gmail.com

## ABSTRACT

Wearable technologies such as smart-glasses can sense, store and display sensitive personal contents. In order to protect this data, users need to securely authenticate to their devices. However, current authentication techniques, such as passwords or PINs, are a poor fit for the limited input and output spaces available on wearables. This paper focuses on eyewear and addresses this problem with a novel authentication system that uses an alphabet of simple tapping patterns optimized for rapid and accurate input on the temples (or arms) of glasses. Furthermore, it explores how an eyewear display can support password memorization by privately presenting a visualization of entered symbols. A pair of empirical studies confirm that performance during input of both individual password symbols and full passwords is rapid and accurate. A follow-up session one week after the main study suggests using a private display to show entered password symbols effectively supports memorization.

## CCS CONCEPTS

• **Security and privacy → Graphical / visual passwords**; • **Human-centered computing → Mixed / augmented reality**;

## KEYWORDS

PIN entry, Security, Visual feedback, Authentication, Smart glasses, Usability, Memorability

**ACM Reference Format:**
MD. Rasel Islam, Doyoung Lee, Liza Suraiya Jahan, and Ian Oakley. 2018. GlassPass: Tapping Gestures to Unlock Smart Glasses. In *AH2018: The 9th Augmented Human International Conference, February 7–9, 2018, Seoul, Republic of Korea.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3174910.3174936


*AH2018, February 7–9, 2018, Seoul, Republic of Korea*

ACM ISBN 978-1-4503-5415-8/18/02…$15.00
https://doi.org/10.1145/3174910.3174936

## 1 INTRODUCTION

Wearable smart glasses are an emerging device category that present many novel interaction challenges [30]. Equipped with large, high resolution and private graphical displays, they are capable of displaying a rich range of contents to their users [36]. Indeed, the fact that the content they show is visible only to a user may make them the ideal platform for display of sensitive or secure information. However, their diminutive input surfaces [11, 19] complicate this issue by making authenticating securely to these devices a challenge. Conventional authentication techniques, such as passwords, require users to accurately enter long, complex strings, a task that is likely to be extremely laborious on a pair of glasses. Even the much simpler PINs require users to enter a sequence of numeric data, an operation that is not directly supported on smart glasses.

A number of factors contribute to this problem. As touch surfaces are necessarily offset from displays, direct touch-screen interaction is not possible [1, 11, 19]. Furthermore, input surfaces, mounted on areas like the arms of glasses, are typically out of sight. This means all input needs to take place eyes-free [1, 11]. Finally, the input surfaces are also small compared to conventional controllers. The Google Glass, for example, features a touch input panel that is 76.2mm by 10.4mm in size [11]. To address these limitations, the standard password entry system on Glass is based on a non-alphanumeric symbol set composed of ten strokes and taps. However, we note that performance assessments of this technique suggest it is slow and cumbersome [35]. In particular, authors report that users find its complex two finger multi-direction swipe gestures to be error-prone. Furthermore, the memorability of passwords using this kind of symbol set is an unknown quantity. Given the well-documented propensity for users to forget alpha-numeric passwords, or to use insecure coping strategies such as password re-use [23], we argue that many users will struggle to memorize this kind of non-standard content.

To address these problems, this paper contributes a novel password scheme designed directly for touch surfaces on the temples (or arms) of glasses. This scheme uses a symbol set of ten different one and two finger tapping gestures. We also contribute an assessment of the viability of this scheme through the results of two empirical studies. The first catalogs basic performance when entering the symbols, while the second explores performance during full password entry. As the symbol set is non-traditional, we also suggest passwords constructed using it may be challenging for users to remember. To deal with this issue, the final contribution of this

paper is the idea of using the private display of smart glasses to present password hints in the form of a persistent visual depiction of entered symbols. We evaluate this idea in the second study by assessing memorability with and without hints both in the initial session and in a follow-up one week later. We also analyze the passwords created by users to explore if there are any systematic biases in symbol selection that would increase their guess-ability and, consequently, lower the resistance of the system to intelligent guessing attacks.

## 2 RELATED WORK

### 2.1 Password/ Authentication Entry Systems

A range of technologies have been proposed to support secure authentication to or with smart-glasses. For example, Chan *et al.* [5] propose a One Time Password (OTP) system that takes advantage of the camera on Google Glasses. In this system, a user generates a QR code on his or her phone, and then scans this with the glasses to authenticate. While this sidesteps problems of making input on the eyewear, it remains a complex process in which interaction with a pair of devices and applications needs to be organized and managed. The feasibility of voice authentication has also been explored [35]. While this technology can combine biometrics (i.e., voice recognition, something you are) with passwords (i.e., something you know), it requires users to speak content out loud, something that may not always be appropriate or comfortable, irrespective of its level of security.

Other authors have proposed taking advantage of private nature of smart glass displays to support shoulder-surfing resistant PIN entry techniques on both mobiles [32] and standalone glasses [4]. The essence of the idea is that private content on eyewear can be used to modulate or transform publicly observable input such that the entered data cannot be used to reconstruct the password. Authors have explored this idea using touches on the screen of a mobile [32] or (via thermal finger tracking) an arbitrary object [9] as well as via strokes on glasses' touchpads and spoken words [4]. The most common approach in this work is to create (and show on the glasses) a new *input-symbol* to *password-item* mapping for every password item entered. In this way, authors separate the observable input from the entered password contents, typically at the cost of raising cognitive complexity and reducing input speed. Regardless, this work highlights the potential of private displays to improve password entry systems.

A final approach to authentication on smart glasses is biometric. This includes vision-based techniques based on traditional techniques such as iris recognition and behavioral ones derived from properties such as changes in pupil size [28] or data derived from head movement patterns in response to musical cues [15]. While biometrics bring many advantages, physical biometrics typically require dedicated sensing hardware and behavioral biometrics can be slow - Li *et al.*s' head movement based system [15] performs best after prolonged input of over ten seconds. Furthermore, problems with reliability over time and across a broad range of input scenarios typically means traditional passwords serve as a backup to biometric authentication - the use of biometrics does not reduce the need for passwords, just lowers the frequency with which they are entered, placing more emphasis on qualities such as the memorability.

A wide variety of novel touch-based authentication mechanisms have also been proposed for other device form factors, such as mobile phones. For example, Azenkot *et al.* [3] proposed a ten-symbol system based on multi-finger chord input designed to facilitate secure authentication by visually impaired users. This system uses the hand-sized touch surface available on a mobile phone to encode a password with spatial patterns of input. Studies suggest it has comparable entropy to standard numeric PINs, while improving on authentication input time for its target visually impaired user group. In the area of touch biometrics [14], authors seek to combine explicit user input, such as button selections, with data about how touches are performed in order to increase confidence about the identity of a user. De Luca *et al.* [6] describe a representative project that combines data about the start and end points of strokes made on the screen of on a mobile phone screen with time sequence data captured during their performance. They show that combining this data can help to reliably identify users.

### 2.2 Input on Wearables

There is also a thriving research community designing and evaluating novel input systems for smart glasses. A key focus is on improving input on touch surfaces integrated into glasses. Much of the work in this area has focused on the demanding topic of text entry. For example, SwipeZone [11] divides the side-mounted touch pad on Google Glass into three zones. Taps and vertical swipes in each zone provide a total of nine possible rapidly executable inputs (mean 150ms) that can be used to control a T9 text entry system capable of achieving 8.73 WPM with a 6% error rate. Similarly, Yu *et al.* [36] present one-dimensional handwriting, a Google Glass text entry system based on 26 unique forward-backward strokes that achieves between 4.67 WPM (character level) and 19.6 WPM (word level, expert use); mean on-screen gesturing time for individual strokes was reported to be 504ms. Gugenheimer *et al.* [12] provide a more general study of the value of on-headset touch input through studies cataloging and comparing, among other things, speed and accuracy on sensor surfaces mounted on both the side and front of a VR headset. Their data indicates input is relatively rapid ( 1500ms) and accurate (2%-6%), with input on the side of the device incurring a performance hit due to the touch surface being offset from the displayed VR contents.

Another common approach to touch input on glasses is to design novel controllers and integrate them into or onto other body locations. For example, Dobbelstein *et al.* [7] propose a touch sensitive belt to control an AR display and report on social acceptability of using such a system - quick touches (2-4 seconds) are acceptable on most of the device surface but more sustained contact should be restricted to the areas above the front trouser pockets. Wang *et al.* [26] describe a typing system involving superimposing a keyboard over the palm and fingers of one hand and making selections with the index finger of the other. With a high-end tracking system a WPM of up to 7.66 can be achieved; with an IR based wrist mounted tracker this drops to 4.6. Finally, Ahn *et al.* [1] study the use of a modified smartwatch as an input system for glasses in a typing task. They report that WPM of up to 10.8 can be achieved in

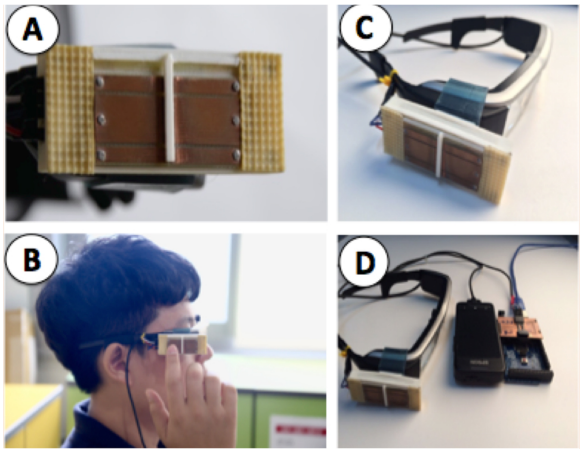


**Figure 1: GlassPass prototype. PCB divided into two touch areas by a centrally positioned raised plastic ridge (A). Finger touching the sensors as trials are shown on screen of Epson Moverio BT-200 glass (B). The prototype mounted on smart glasses (C) and the touchpad sensors connected with an Arduino Mega 2560 (D).**

optimal conditions. Gestures are also a staple of AR input systems and numerous systems have been proposed exploring the design or implementation of hand [25] or foot [16] gestures using techniques such as visual tracking or through dedicated sensing hardware in wearables such as gloves [13]. An issue underlying much of this work is the social acceptability of gestural input.

Tapping gestures have also been previously explored on wearables. The Beats system [17] for smartwatches presents a system of sequential and/or simultaneous finger tapping gestures and characterizes time for distinguishing between these inputs. This concept and the timing threshold influenced the design of the tapping gesture set proposed in this paper.

## 3 GLASSPASS HARDWARE PROTOTYPE

In order to explore tapping and touch gestures on smart glasses, we opted to construct a bespoke touch sensor for a pair of Epson Moverio BT-200 AR glasses. This was due to the relatively large display (23°) available on this platform and the fact that we wanted to sense not only touches, but also the size or shape of those touches. The sensor is shown Figure 1(B) and 1(C). It features six capacitive electrodes arranged in a two by three grid on a custom PCB connected to a Sparkfun MPR121 breakout board and interfaced via a cable to an Arduino. The top and bottom electrodes of the PCB were in similar size (height 3.5 mm) while the middle electrodes were larger (10 mm). All electrodes were 16mm wide. A raised 1.5 mm thick spacer separated the left and right blocks. The goal of this arrangement was to reliably sense touches to the left and right columns, and also to distinguish between taps made with the finger-tip and those made with the flat of the finger. To achieve this, the spacing of the sensors was designed for a finger-tip tap to come into contact with at most two electrodes and a finger flat tap to touch all three (see Figure 1(C)).

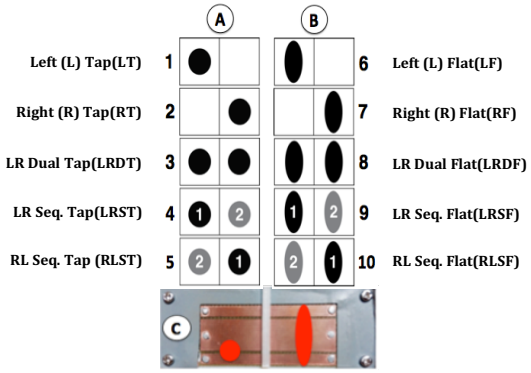


**Figure 2: Designed ten gestures, five fingertip taps (A), five finger flat taps gestures (B) and the gesture making process (C).**

The sensor unit fit inside a 64 mm by 25.5 mm by 8 mm 3D printed case. The area immediately to the left and right of the PCB was covered by a rough textured rubber to provide tactile cues to distinguish between the touch area and its surrounds and support eyes-free use. All graphical contents in the studies were displayed on the Android Epson Moverio BT-200 eyewear.

## 4 STUDY-1: USER VALIDATION STUDY

This initial study was designed to assess system reliability and the speed and accuracy with which participant were able to enter tapping gestures on its surface. For this study, we designed a set of ten gestures, illustrated in Figure 2. Five gestures used finger-tip taps and five used finger-flat taps. Each subset of five was composed of the following mixture of left and right inputs (corresponding to taps made with the index and middle fingers): a single tap with the index finger; a single tap with the middle finger; a simultaneous tap with both fingers; a sequential tap of index followed by middle finger and; a sequential tap of middle followed by index finger. To register the sequential touches, the first finger needed to remain on the sensor until the second finger makes contact. This structure effectively disambiguates sequential touches from sequences of single touches. The timing threshold to differentiate between simultaneous and sequential touches was 30ms [17].

The study had a simple, single condition structure. It was composed of three sessions, each featuring 15 repetitions of the ten gestures delivered in a random order. The first session was treated as practice and not analyzed. In each trial participants were first requested to tap the sensor to start. A fixation spot was then presented until one second after participants released the sensor, followed by one of the symbols from Figure 2. The user was then required to enter the corresponding symbol and received feedback as to correctness (a red cross or green tick) after releasing the sensor. Participants were required to repeat erroneously completed gestures. We logged the start and end time of each touch to the sensor as well as the error rate. We defined the trial touch time as the total duration of time any finger was in contact with the sensor.

The experiment was conducted in a quiet office room with participants seated in front of a desk on a height adjustable chair.

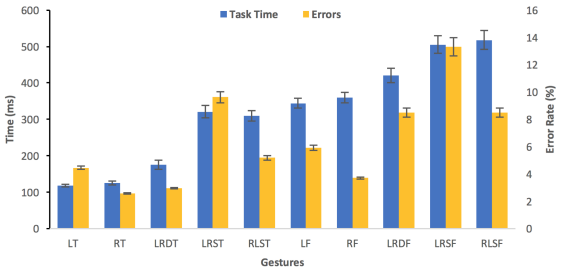


**Figure 3: Mean touch time and errors from the ten different taps in the validation study. Bars show standard error.**

Participants rested their right elbow on the experiment table to aid in keeping their fingers in a comfortable position over the touch sensor. Nine right-handed participants (4 female) with a mean age of 24 years participated in the study. Participants were recruited from an on-line university social media group. All the participants were either undergraduate or graduate students at UNIST with high smartphone and touchscreen experience (4.3/5) but low smart eyewear experience (1.2/5). The validation experiment took about 30 minutes and participants were compensated with approximately 10 USD.

## 4.1 Results

The mean touch time for all gestures was 319ms. This data is broken down by gesture in Figure 3. A one way repeated measure ANOVA, incorporating Greenhouse-Geisser corrections and treating gesture as an independent variable confirmed that touch times differed significantly among the gestures ($F(1, 8)=176.529$, $p<0.001$). This is not surprising: some of the gestures involved simple single taps, while others involved compound movements of two fingers. Due to this fact and as we had no specific hypotheses about the differences between the different gestures, we opted not to run post-hoc tests on this data; the chart clearly illustrates that time increases with input complexity. We note that mean performance of this set is relatively high. For example, in their discussion of the stroke based gesture set for One-Dimensional Handwriting, Yu *et al.* [36], report a mean gesture time (corresponding to our touch time) of 504ms. Our symbol set is able to improve on this considerably, most likely because of its smaller cardinality: a smaller range of possible inputs let us select simpler primitives that can be more rapidly performed. Error data are shown in Figure 3; the mean is 6.6%. Another RM ANOVA revealed a significant trend ($F(1, 8) = 19.780$, $p=0.002$). As differences were less clear, we ran post-hoc t-tests incorporating Bonferroni corrections to identify specific differences; none attained significance. As such, we conclude that although the 10 tapping gestures represent movements of differing complexity (that take different amount of times to execute), all can be performed sufficiently reliably to form part of a password entry symbol set.

# 5 STUDY-2: PASSWORD STUDY

Encouraged by the results of the validation study, we conducted a more substantial evaluation of the use of the tapping symbol set as passwords. We created a simple password creation system

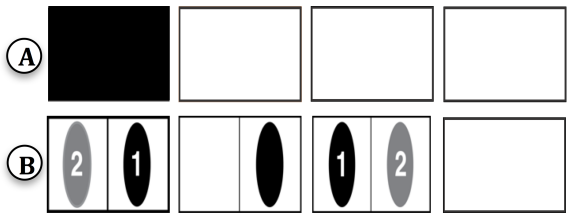


**Figure 4: Feedback in password entry bars in study 2. (A) shows standard feedback condition: user input is marked by black highlights for each password item entered. (B) shows disclosed condition: as users input their password the symbols are displayed on the private glasses display(B). (A) shows password bar after a single entry, while (B) shows bar after three entries.**

on a PC that allowed users to choose (or be assigned) a tapping password and altered the software on the Epson glasses to support the entry of a password composed of four consecutive password items delimited by sensor releases. We then evaluated performance with this system against two binary variables: password-type, referring to whether participants chose their own passwords or had a password assigned by the experimenters, and feedback, related to the type of cues displayed on the private glasses display. We investigated the difference between *assigned* and *chosen* passwords to understand if there were biases in users' password selection processes and to determine whether or not self-selected passwords were more memorable than assigned ones. Prior work has used similar approaches to investigate password memorability and security issues by contrasting user generated and system-assigned passwords [2, 8, 22, 23, 33]. The symbols in the assigned passwords were balanced such that they, on aggregate, covered the entire symbol set equally. Specifically, the 12 participants who were assigned passwords required a total of 48 symbols - eight of the GlassPass symbols was used ten times, with the remaining two used four times. Beyond this constraint, symbol assignment to passwords was random.

We defined two systems for the feedback variable: a *standard* password entry feedback bar in which each additional entered character is marked with a highlight (see Figure 4(A)) and a *disclosed* version of this feedback in which the entered symbols are visually displayed as they are input (see Figure 4(B)). We argue the disclosed system is secure as the glasses display is private and not susceptible to attacks such as in-person or camera based shoulder surfing [32]. The motivation for including the disclosed feedback is to facilitate memorization and recall of the password through visual exposure to a representation of its contents. In a password composed of an unusual symbol set of taps, we believe this kind of memory aid could help alleviate problems with password recall.

## 5.1 Experimental Description and Design

Twenty-four right-handed participants (13 female, mean age 25) participated in the password study. The study followed a between groups design with six participants per group and each group completing one of the four conditions. Each participant finished two

sessions: a full study of the password entry system and a brief memorability session one week later. Participants were compensated with 15 USD in local currency for the first session and 10 USD for the second. No participant dropped out between the two sessions.

The password study started with a familiarization session. An experimenter first demonstrated the ten input symbols. Participants then completed a short session of 15 repetitions of the ten symbols delivered in a random order. This was to gain familiarity with the input system. The password study then began with the participant creating or being assigned a password, depending on the experimental condition. This password was used for the participant throughout the remainder of the study. There were then six input sessions, each including ten repetitions of full entry of the participant's four-item password. The first two sessions were considered practice and discarded. The remaining four sessions (40 trials) were retained for analysis. This resulted in a data set of 24*40*4 = 3840 individual password symbol entries. At the end of each of the six sessions, participants were encouraged to rest for as long as they wanted. In this study, we measured password entry time, defined as the full time it took to enter a four-item password. Incorrect trials were also logged at the password level (e.g. one erroneous symbol corresponds to an erroneous password) and subjective workload was measured via the NASA TLX.

Immediately after completing the password study we assessed short-term password memorability. Participants first played a card matching game on a mobile device for five minutes to occupy their working memory. They then entered their password again, following the common protocol of being given three chances [2] to enter it correctly. The follow-up memorability session was conducted one week after the main study. This is a time interval commonly used in authentication studies assessing memorability [2, 22]. The study took the same form: participants donned the glasses and had three chances to enter their password. In order to reduce the chances that participants would adopt strategies such as noting down passwords immediately after the first study, we provided no information about the nature of the follow up session during the first session.

## 5.2 Results

All analyses, unless otherwise mentioned, were two-way ANOVAs. Error rates are shown in Figure 5(C). Neither the interaction ($F(1, 20) = 1.25$, $p>0.05$) nor the main effects of password-type ($F(1, 20) = 1.25$, $p>0.05$) or feedback ($F(1, 20) = 1.25$, $p>0.05$) led to significant differences. Examining the raw data, it shows a clear uniform trend. Consequently, we can conclude that assigned passwords, with their more diverse symbol set, are as reliable to enter as chosen ones. Password entry time data are shown in Figure 5(B). The ANOVA on password entry time also showed no significant interaction ($F(1, 20) = 0.23$, $p>0.05$) nor main effect of feedback ($F(1, 20) = 0.006$, $p>0.05$). However, the password-type variable attained significance ($F(1, 20) = 5.198$, $p<0.05$) indicating that users entered their passwords more quickly if they had chosen the password themselves. This likely reflects the composition of symbols in the passwords and reflects a propensity for users to select password symbols they believe are simpler and quicker to enter. We discuss this issue in more detail in section 6.

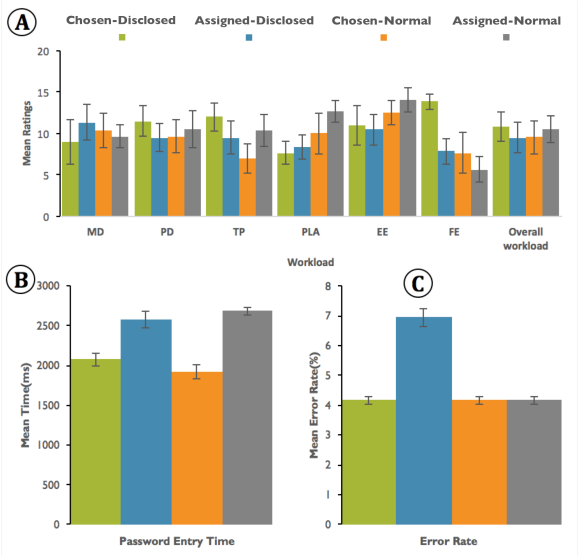


**Figure 5: Mean password entry time, errors, and TLX subjective data from the four conditions of password study. Bars show standard error.**

Workload data are presented in Figure 5(A). Given the high variance and proximate means in this data set, we opted not to conduct a factor by factor analysis. Instead, we calculated overall workload and tested for differences on this aggregate score. There are no significant differences in the interaction ($F(1, 20) = 1.67$, $p>0.05$) or main effects of password-type ($F(1, 20) = 0.05$, $p>0.05$) and feedback ($F(1, 20) = 0.04$, $p>0.05$). This suggests that neither the presence or absence of feedback, nor the requirement to use a created or assigned password had a measurable impact on the workload experienced in the study.

We made two assessments of password memorability. The first took place immediate after participants completed the training study and a distracter task intended to occupy their working memory so they would not be able to continuously attend to their password contents. The second took place in a follow-up study session one week after the main study. We were careful not to forewarn participants as to the purpose of the second study to prevent behaviors such as noting down or otherwise working to thoroughly memorize their passwords. In the initial memorability assessment, two participants in the chosen-standard condition failed to enter their passwords at the first attempt. Both succeeded on the second attempt. While these errors may represent failures of memory, they could also be attributed to data input errors - two failures from 24 participants would amount to an 8.3% error rate, roughly consistent with the error rate recorded in the study as a whole.

Results from the session one week later are more conclusive. Two participants from the chosen-standard and two participants from the assigned-standard groups entirely failed to enter their passwords on all three attempts. All reported not being able to remember their passwords. In both of the disclosed conditions, however, all participants correctly entered their passwords at the first attempt. Although this evidence is from a relatively small

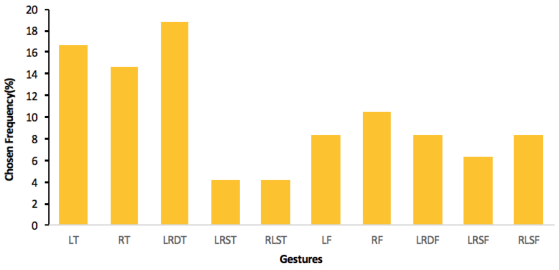


**Figure 6: Symbol frequency ratios (%) used by participants in the chosen password condition. The four single taps were used 24 times (50%), the two dual taps were used 13 times (27.08%) and the four sequential taps were used 11 times (22.92%).**

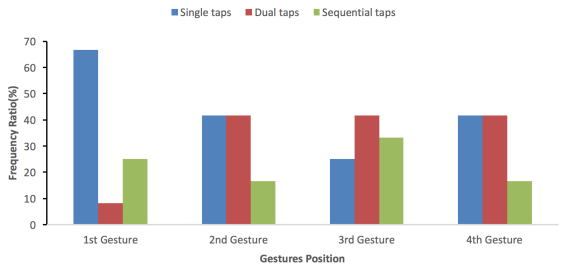


**Figure 7: Frequency of each type of tap (single, dual and sequential) used in each password item (first through fourth).**

participant pool, it is sufficiently strong (1/3 of participants in the standard condition failed to remember their passwords vs none in the disclosed condition) to suggest that there are benefits to using a private display to provide password hints in the form of a visualization of entered input.

At the end of both study sessions, participants were given the opportunity to present their comments and opinions about the system. Comments from those in the disclosed conditions support our assertion that the feedback was valuable. In a representative statement, P16 remarked that having the symbols on screen was an effective memory aid. Participants were more split about the memorability of the tapping gesture set in general. Some participants reported that the rhythmic qualities of the interaction made it easy to remember the password (their "fingers remembered" (P9)) while others found the symbols abstract: "[flat] gestures are difficult to remember" (P21) and "confusing" (P18).

## 6 GLASSPASS SECURITY

This section explores the security of the GlassPass in terms of the strength of the passwords participants generated. In this analysis, we consider only the 12 users in the chosen group. Figure 6 shows the frequency of GlassPass symbols selected, showing a tendency to choose single or dual taps over other symbols. Conversely, sequential taps were used much more infrequently - the four possible inputs were selected just 23% of the time. Figure 7 breaks down this data into the inputs used for each item in the password showing the preference for single taps is particularly prevalent when choosing the first input in a GlassPass password - 60% of first items were single taps. In subsequent password items, distributions were more even, although participants still under-used sequential taps. This suggests that password policies would be required to encourage users to deploy sequential taps in order to ensure that GlassPass passwords are resistant against informed brute force or guessing attacks.

We also analyzed the generated password to determine if the use of repeated symbols (e.g. 1122 in a numeric PIN) was common. These types of repetition weaken the security of passwords by increasing guess-ability based on rule-based attacks. We examined repetition in the following six patterns, where "X" denotes a repeated item and "?" any other item: XX??, X?X?, X??X, ?XX?, ?X?X, ??XX. Surprisingly, just one password contained a single incidence of repetition (in the format XX??), suggesting that GlassPass would be resilient to attacks that seek to exploit rule based repetition. We suggest this may be due to the fact that GlassPass input is non-numeric and non-lexical. As it is not anchored on an established alphabet, participants saw few benefits in using repetition to help them learn, remember or produce their passwords.

## 7 DISCUSSION

Performance with the GlassPass system was generally high: passwords were entered rapidly (2300ms) and with an acceptable reliability of 95%. This offers improvements over prior entry systems for eyewear that focus on stroke gestures rather than tapping gestures [11]. Specifically, our system is 2.43 times as fast as entry times reported for the standard stroke authentication that shipped on the Google Glass - Yadav *et al.* report this to be 5589ms [35]. Furthermore, the password entry times are relatively close to the standard times for regular four-digit PIN entry on a numerical keyboard - typically reported to be in the 1-2 second range [32]. As such high performance is the result of consistent practice, we find it highly encouraging that the tapping gesture set in this paper can approach this level of input efficiency. As such, we believe our study supports the use of tapping gestures for eyewear in situations where there are a limited number of possible symbols in the input set.

It is worth further contrasting performance with GlassPass against alternative input systems and approaches to authentication on smart glasses. In terms of behavioral biometrics, Li *et al.* [15] report an Equal Error Rate (EER) of 4.43% after 10 seconds of motion input. In GlassUnlock [32], where the glass display is used to present content that obfuscates the meaning of physical input on a phone, entry times are 4.8 to 4.9 seconds with a mean accuracy of 5.22%. The authors partly attribute the protracted entry times to the requirement for repeated shifts of visual attention from glasses to phone. Finally, data from studies of FaceTouch [12] suggest that while blind target selections on the side of a device are highly inaccurate (error rate of 64% for select on finger down), performance improves to 4% if users are allowed to adjust targeting interactively before selecting on release. We again highlight that GlassPass offers performance improvements over these approaches in terms of its

speed (2300ms) and/or error rate (5%). We attribute these advantages to GlassPass's focus on eyes-free input that is specifically designed for rapid performance on small touchpads.

We also argue that GlassPass presents benefits in terms of password memorability. Although the evaluation is limited in scope to a single longitudinal assessment, the results support the idea that the private displays of smart glasses can be used to aid in secure password memorization though the simple approach of displaying entered symbols. This recommendation has the benefit of being trivial to implement in current systems (requiring only a software update) and is applicable to any type of password system, including those based on traditional alphanumeric characters. We argue that password forgetting is a major problem [29] that a simple aid such as persistently displaying feedback about entered information can help address.

GlassPass has a number of limitations. One potential problem is its reliance on capturing the shape of finger contact regions. While this is an established (e.g., [18, 20, 21, 24, 27, 31]) form of input in the research community, it is one that remains relatively uncommon in current consumer devices. However, given that recent research is implementing shape detection functionality by hacking the software on consumer wearables such as watches [10, 34], we believe that it is realistic to expect that future glass systems will be able to capture the kind of touch data required for GlassPass input. A related issue is the relatively large size of the GlassPass touch input system. While its horizontal length is similar to commercial systems such as Google Glass (76.2mm long), it is relatively large vertically (18mm compared to 10.4). Further work is required to investigate if the GlassPass input technique is effective on smaller touch surfaces that might be more practically integrated into eyewear. Additionally, although we present an analysis of the how users select password items to examine if biases are present, the sample size of the current study makes this speculative and inconclusive; a larger scale study would need to study this issue in more depth. Finally, there are a number of common threat models that GlassPass does not consider. Perhaps the most prominent of these is observation - either by shoulder surfing or via camera. Future work will seek to adapt GlassPass to incorporate input mappings that leverage the personal glass screen to obfuscate observable physical inputs to improve resistance to attacks of this form [32].

## 8 CONCLUSIONS

In conclusion, we believe that next generation smart eyewear will store, show and manipulate all sorts of sensitive user information. Securing access to these devices is therefore important. However, to ensure that users opt to deploy security measures, research is needed to create systems that appropriately combine security with usability. GlassPass achieves this in several critical ways. Firstly, it maintains the entropy, or available password space, of a standard ATM PIN. Secondly, it supports rapid and reliable input. Thirdly, it integrates a simple technique to increase password memorability. We believe techniques such as GlassPass can be directly integrated into next generation smart glasses.

## ACKNOWLEDGMENTS

We would like to thank all our study participants. This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning ( 2017R1D1A1B03031364).

## REFERENCES

[1] Sunggeun Ahn, Seongkook Heo, and Geehyuk Lee. 2017. Typing on a Smartwatch for Smart Glasses. In *Proceedings of the 2017 ACM International Conference on Interactive Surfaces and Spaces (ISS '17)*. ACM, New York, NY, USA, 201–209. https://doi.org/10.1145/3132272.3134136

[2] Mahdi Nasrullah Al-Ameen, Matthew Wright, and Shannon Scielzo. 2015. Towards Making Random Passwords Memorable: Leveraging Users' Cognitive Ability Through Multiple Cues. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2315–2324. https://doi.org/10.1145/2702123.2702241

[3] Shiri Azenkot, Kyle Rector, Richard Ladner, and Jacob Wobbrock. 2012. PassChords: Secure Multi-touch Authentication for Blind People. In *Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '12)*. ACM, New York, NY, USA, 159–166. https://doi.org/10.1145/2384916.2384945

[4] Daniel V Bailey, Markus Dürmuth, and Christof Paar. 2014. "Typing" passwords with voice recognition: How to authenticate to Google Glass. In *Proc. of the Symposium on Usable Privacy and Security*.

[5] Pan Chan, Tzipora Halevi, and Nasir Memon. 2015. *Glass OTP: Secure and Convenient User Authentication on Google Glass*. Springer Berlin Heidelberg, Berlin, Heidelberg, 298–308. https://doi.org/10.1007/978-3-662-48051-9_22

[6] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. 2012. Touch Me Once and I Know It's You!: Implicit Authentication Based on Touch Screen Patterns. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. ACM, New York, NY, USA, 987–996. https://doi.org/10.1145/2207676.2208544

[7] David Dobbelstein, Philipp Hock, and Enrico Rukzio. 2015. Belt: An Unobtrusive Touch Input Device for Head-worn Displays. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2135–2138. https://doi.org/10.1145/2702123.2702450

[8] Alain Forget, Sonia Chiasson, P. C. van Oorschot, and Robert Biddle. 2008. Improving Text Passwords Through Persuasion. In *Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS '08)*. ACM, New York, NY, USA, 1–12. https://doi.org/10.1145/1408664.1408666

[9] G. Gheorghe, N. Louveton, B. Martin, B. Viraize, L. Mougin, S. Faye, and T. Engel. 2016. Heat is in the eye of the beholder: Towards better authenticating on smartglasses. In *2016 9th International Conference on Human System Interactions (HSI)*. 490–496. https://doi.org/10.1109/HSI.2016.7529679

[10] Hyunjae Gil, DoYoung Lee, Seunggyu Im, and Ian Oakley. 2017. TriTap: Identifying Finger Touches on Smartwatches. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 3879–3890. https://doi.org/10.1145/3025453.3025561

[11] Tovi Grossman, Xiang Anthony Chen, and George Fitzmaurice. 2015. Typing on Glasses: Adapting Text Entry to Smart Eyewear. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '15)*. ACM, New York, NY, USA, 144–152. https://doi.org/10.1145/2785830.2785867

[12] Jan Gugenheimer, David Dobbelstein, Christian Winkler, Gabriel Haas, and Enrico Rukzio. 2016. FaceTouch: Enabling Touch Interaction in Display Fixed UIs for Mobile Virtual Reality. In *Proceedings of the 29th Annual Symposium on User Interface Software and Technology (UIST '16)*. ACM, New York, NY, USA, 49–60. https://doi.org/10.1145/2984511.2984576

[13] Yi-Ta Hsieh, Antti Jylhä, Valeria Orso, Luciano Gamberini, and Giulio Jacucci. 2016. Designing a Willing-to-Use-in-Public Hand Gestural Interaction Technique for Smart Glasses. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 4203–4215. https://doi.org/10.1145/2858036.2858436

[14] Lijun Jiang and Weizhi Meng. 2017. *Smartphone User Authentication Using Touch Dynamics in the Big Data Era: Challenges and Opportunities*. Springer International Publishing, Cham, 163–178. https://doi.org/10.1007/978-3-319-47301-7_7

[15] S. Li, A. Ashok, Y. Zhang, C. Xu, J. Lindqvist, and M. Gruteser. 2016. Whose move is it anyway? Authenticating smart wearable devices using unique head movement patterns. In *2016 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. 1–9. https://doi.org/10.1109/PERCOM.2016.7456514

[16] Zhihan Lv, Alaa Halawani, Shengzhong Feng, Shafiq ur Réhman, and Haibo Li. 2015. Touch-less interactive augmented reality game on vision-based wearable device. *Personal and Ubiquitous Computing* 19, 3 (01 Jul 2015), 551–567. https://doi.org/10.1007/s00779-015-0844-1

[17] Ian Oakley, DoYoung Lee, MD. Rasel Islam, and Augusto Esteves. 2015. Beats: Tapping Gestures for Smart Watches. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1237–1246. https://doi.org/10.1145/2702123.2702226

[18] Ian Oakley, Carina Lindahl, Khanh Le, DoYoung Lee, and MD. Rasel Islam. 2016. The Flat Finger: Exploring Area Touches on Smartwatches. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 4238–4249. https://doi.org/10.1145/2858036.2858179

[19] Ge Peng, David T. Nguyen, Gang Zhou, and Shuangquan Wang. 2015. Poster: A Continuous and Noninvasive User Authentication System for Google Glass. In *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '15)*. ACM, New York, NY, USA, 487–487. https://doi.org/10.1145/2742647.2745906

[20] Simon Rogers, John Williamson, Craig Stewart, and Roderick Murray-Smith. 2011. AnglePose: Robust, Precise Capacitive Touch Tracking via 3D Orientation Estimation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 2575–2584. https://doi.org/10.1145/1978942.1979318

[21] Anne Roudaut, Eric Lecolinet, and Yves Guiard. 2009. MicroRolls: Expanding Touch-screen Input Vocabulary by Distinguishing Rolls vs. Slides of the Thumb. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*. ACM, New York, NY, USA, 927–936. https://doi.org/10.1145/1518701.1518843

[22] Richard Shay, Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Blase Ur, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2012. Correct Horse Battery Staple: Exploring the Usability of System-assigned Passphrases. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. ACM, New York, NY, USA, Article 7, 20 pages. https://doi.org/10.1145/2335356.2335366

[23] Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2010. Encountering Stronger Password Requirements: User Attitudes and Behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*. ACM, New York, NY, USA, Article 2, 20 pages. https://doi.org/10.1145/1837110.1837113

[24] Brandon T. Taylor and V. Michael Bove, Jr. 2009. Graspables: Grasp-recognition As a User Interface. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*. ACM, New York, NY, USA, 917–926. https://doi.org/10.1145/1518701.1518842

[25] Ying-Chao Tung, Chun-Yen Hsu, Han-Yu Wang, Silvia Chyou, Jhe-Wei Lin, Pei-Jung Wu, Andries Valstar, and Mike Y. Chen. 2015. User-Defined Game Input for Smart Glasses in Public Space. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 3327–3336. https://doi.org/10.1145/2702123.2702214

[26] Cheng-Yao Wang, Wei-Chen Chu, Po-Tsung Chiu, Min-Chieh Hsiu, Yih-Harn Chiang, and Mike Y. Chen. 2015. PalmType: Using Palms As Keyboards for Smart Glasses. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '15)*. ACM, New York, NY, USA, 153–160. https://doi.org/10.1145/2785830.2785886

[27] Feng Wang, Xiang Cao, Xiangshi Ren, and Pourang Irani. 2009. Detecting and Leveraging Finger Orientation for Interaction with Direct-touch Surfaces. In *Proceedings of the 22Nd Annual ACM Symposium on User Interface Software and Technology (UIST '09)*. ACM, New York, NY, USA, 23–32. https://doi.org/10.1145/1622176.1622182

[28] T. Wang, Z. Song, J. Ma, Y. Xiong, and Y. Jie. 2013. An anti-fake iris authentication mechanism for smart glasses. In *2013 3rd International Conference on Consumer Electronics, Communications and Networks*. 84–87. https://doi.org/10.1109/CECNet.2013.6703278

[29] Roman Weiss and Alexander De Luca. 2008. PassShapes: Utilizing Stroke Based Authentication to Increase Password Memorability. In *Proceedings of the 5th Nordic Conference on Human-computer Interaction: Building Bridges (NordiCHI '08)*. ACM, New York, NY, USA, 383–392. https://doi.org/10.1145/1463160.1463202

[30] Jens Weppner, Andreas Poxrucker, Paul Lukowicz, Shoya Ishimaru, Kai Kunze, and Koichi Kise. 2014. Shiny: An Activity Logging Platform for Google Glass. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp '14 Adjunct)*. ACM, New York, NY, USA, 283–286. https://doi.org/10.1145/2638728.2638798

[31] Daniel Wigdor, Hrvoje Benko, John Pella, Jarrod Lombardo, and Sarah Williams. 2011. Rock & Rails: Extending Multi-touch Interactions with Shape Gestures to Enable Precise Spatial Manipulations. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 1581–1590. https://doi.org/10.1145/1978942.1979173

[32] Christian Winkler, Jan Gugenheimer, Alexander De Luca, Gabriel Haas, Philipp Speidel, David Dobbelstein, and Enrico Rukzio. 2015. Glass Unlock: Enhancing Security of Smartphone Unlocking Through Leveraging a Private Near-eye Display. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1407–1410. https://doi.org/10.1145/2702123.2702316

[33] Nicholas Wright, Andrew S. Patrick, and Robert Biddle. 2012. Do You See Your Password?: Applying Recognition to Textual Passwords. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. ACM, New York, NY, USA, Article 8, 14 pages. https://doi.org/10.1145/2335356.2335367

[34] Robert Xiao, Julia Schwarz, and Chris Harrison. 2015. Estimating 3D Finger Angle on Commodity Touchscreens. In *Proceedings of the 2015 International Conference on Interactive Tabletops & Surfaces (ITS '15)*. ACM, New York, NY, USA, 47–50. https://doi.org/10.1145/2817721.2817737

[35] Dhruv Kumar Yadav, Beatrice Ionascu, Sai Vamsi Krishna Ongole, Aditi Roy, and Nasir Memon. 2015. *Design and Analysis of Shoulder Surfing Resistant PIN Based Authentication Mechanisms on Google Glass.* Springer Berlin Heidelberg, Berlin, Heidelberg, 281–297. https://doi.org/10.1007/978-3-662-48051-9_21

[36] Chun Yu, Ke Sun, Mingyuan Zhong, Xincheng Li, Peijun Zhao, and Yuanchun Shi. 2016. One-Dimensional Handwriting: Inputting Letters and Words on Smart Glasses. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 71–82. https://doi.org/10.1145/2858036.2858542