Design and Analysis of Shoulder Surfing Resistant PIN based Authentication Mechanisms on Google Glass

Dhruv Kumar Yadav[1], Beatrice Ionascu[2], Sai Vamsi Krishna Ongole[3], Aditi Roy[3], and Nasir Memon[2,3]

[1] Indian Institute of Technology Kanpur, Kanpur, India
dhruvkr@iitk.ac.in
[2] New York University Abu Dhabi, Abu Dhabi, United Arab Emirates
bi305@nyu.edu
[3] New York University, Polytechnic School of Engineering, Brooklyn, NY, USA
{svo214, ar3824, memon}@nyu.edu

Abstract. This paper explores options to the built-in authentication mechanism of the Google Glass which is vulnerable to shoulder surfing attacks. Two simple PIN-based authentication techniques are presented, both of which provide protection against shoulder surfing. The techniques employ two interfaces for entering the PIN, namely, voice (Voice-based PIN) and touchpad (Touch-based PIN). To enter the same PIN, user has the freedom to choose either technique and thereby interface, as per the environment in which authentication is being performed. A user study was conducted with 30 participants to compare the performance of the proposed methods with the built-in technique. The results show that the proposed mechanisms have a significantly better login success rate than the built-in technique. Interestingly, although the average authentication times of the proposed methods are higher than that of the built-in one, the users perceived them as being faster. The results also indicate that the proposed methods have better perceived security and usability than the built-in method. The study reveals that when it comes to authentication on augmented reality devices, there is a need for authentication mechanisms that complement each other as users tend to prefer a different interface in different contexts.

Keywords: Google Glass, PIN, Authentication, Security, Usability

1 Introduction

Wearable computing devices like the Google Glass [1] are becoming increasingly popular in health-care applications [2]-[4] and there is a promise of growing adoption in many other innovative applications [5], [6]. As with any personal computing device, in order to deter theft and protect personal information, there is a need for an authentication mechanism that binds the specific user to the Glass [7].

In order to authenticate the device user, Google Glass offers a touchpad based pattern lock mechanism. The password is a sequence of four touch gestures chosen from a set of ten gestures, thereby providing the same number of possible passwords as a 4 digit PIN. The gesture set consists of tap or swipe gestures using one or two fingers (see

Figure 1). The user interface for password entry is shown in Figure 2(a), where the three entered gestures are tap, two-finger tap and swipe back.

The key advantage of the built-in technique is that it is universal in the sense that it can be employed in different ambient conditions including noisy and poorly lit environments. A free hand and a sense of touch is all that is needed. However, the technique has some limitations. First, it is susceptible to shoulder surfing, as the sequence of finger movements on the touchpad located on right side of the head is easily visible to others. Second, some of the gestures (specifically the ones involving the hook swipe gesture) require complicated hand movements and are difficult to perform. Finally, the built-in technique does not exploit the full capabilities of this head mounted device where the screen is only visible to the user.

This paper explores the design and usability of two PIN-based authentication mechanisms that are easy to use while providing reasonable security against shoulder surfing unlike the built-in mechanism offered by Google. The techniques are novel in the sense that two different interfaces can be used to enter the PIN, voice and touch, depending on user choice and the external environment. For *Voice-based PIN* (VBP) entry, a user utters a cipher PIN corresponding to the actual PIN. It should be noted that voice is the natural choice of interface for entering the PIN in a wearable headset device like the Google Glass where textual input is provided by voice. Also, the hands-free format of the mechanism makes it ideal for the device. However, the drawbacks of natural language voice commands, specifically noisy background, prevents it from being used in all contexts. To account for such situations, the other interface through which the Google Glass is controlled, i.e. touchpad, can be employed. Thus, we introduce a second technique, namely *Touch-based PIN* (TBP), which complements the VBP. Both of the techniques leverage the private display visible only to the user to provide protection against shoulder surfing. Although, it could be argued that the display of the Glass is not completely private because the screen is visible from the other side. However, the screen is too small for an adversary to read without being strikingly close to the user or using sophisticated camera equipment. The adversary would have to record and post-process the screen (and also the cipher PIN uttered by the user in the case of VBP) to determine the PIN. This is an unrealistic threat for the average Glass user and thus goes beyond the purpose of this paper.

A user study with 30 participants was conducted to evaluate the security, usability, efficiency, and likability of the proposed authentication mechanisms with respect to the built-in authentication technique. From the user's point of view, any authentication mechanism is bound to fail if perceived as complex or time consuming or vulnerable by the user even though it it is theoretically resilient. With this in mind it is important to access the perception of security. In this work, experience of the user is investigated and quantified using System Usability Scale (SUS) assessment [27]. To the best of our knowledge, this work is the first to explore alternative authentication mechanisms on the Google Glass with an extensive user study.

The main contributions of the paper are as follows:

– Design of alternate PIN-based password schemes on Google Glass using either voice or touchpad input.

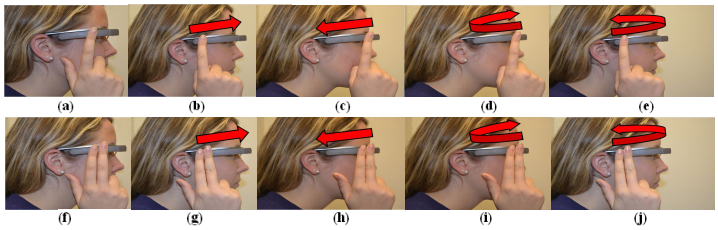

Fig. 1. Available gesture set in the built-in authentication mechanism: (a) tap (b) swipe forward (c) swipe back (d) hook swipe forward (e) hook swipe back (f) two-finger tap (g) two-finger swipe forward (h) two-finger swipe back (i) two-finger hook swipe forward (j) two-finger hook swipe back

- Quantitative evaluation of efficiency and effectiveness of the PIN-based authentication mechanisms along with the built-in one in terms of login time and login success rate, respectively.
- Qualitative evaluation of the three authentication mechanisms in terms of perceived security, usability, and likelihood of future use.
- Analysis of user reaction and preference in different usage contexts.

Results show that VBP and TBP have a higher perceived security and usability than the built-in method. VBP and built-in methods have comparable login times but TBP requires longer time. However, performance of users improved with number of trials. The study also reveals that users prefer different mechanisms in different contexts. They picked either VBP or TBP over the built-in mechanism in public settings.

The rest of the paper is organized as follows. Section 2 discusses existing authentication mechanisms for various user interfaces. In Section 3, the PIN-based authentication schemes are introduced. Section 4 presents the user study design. Evaluation results are presented in Section 5. Detailed interpretation of the results is done in Section 6 and Section 7 concludes the paper.

2 Related Work

Personal identification number (PIN) [9] is the most common user authentication method to prevent unauthorized access in modern hand-held computing devices like mobile phones, tablet, etc. Although in recent times, some devices have incorporated finger-print authentication due to its uniqueness, accuracy, speed and robustness, the mechanism is unlikely to make large impact due to extra cost, additional hardware, non-replaceable nature and fear of identity theft [10]. However, based on short term and lab studies (e.g. [11]), it has been argued that PIN has low memorability and security. To address these issues, multiple methods have been proposed to replace PIN with graphical and pattern-based passwords [12]-[**?**]. However, most of them are not robust enough against various vulnerabilities like shoulder surfing and eavesdropping [9]. Several techniques ([17], [18]) were introduced including hardware based [19]- [21] and biometric feature based ones [22]- [24] to counter these challenges.

With the evolution of touch-screen based devices, the need for authentication mechanisms better suited for such interfaces became evident. Among the previously mentioned schemes, only pattern-based approaches have seen widespread adoption. The drawmetric scheme Draw-a-Secret [14] is implemented in the Android OS as ‘pattern

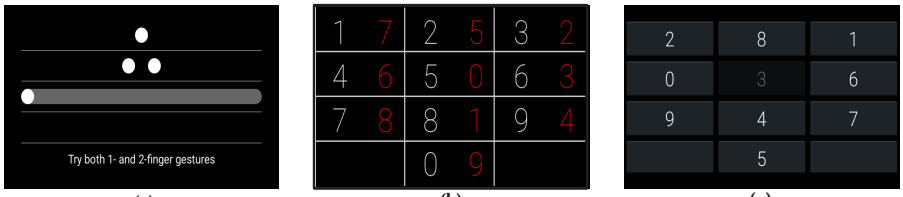

Fig. 2. Layout of the authentication systems. (a) built-in mechanism: the first three entered gestures are tap, two-finger tap, and swipe back (b) VBP mechanism: the white colored digits show the real PIN numbers whereas the red colored digits are the cipher numbers temporarily representing the real PIN digits (c) TBP mechanism: randomly assigned keypad layout that changes with every instance

lock' [25]. However, one recent study in a real world setting over a reasonable period of time shows that PIN outperforms the pattern lock in terms of speed and error rates [26]. Hence, it can be argued that given the threat model and usability constraints, PIN-based authentication is a reasonable alternative, often in combination with another factor, and will be hard to replace.

The approaches discussed above were designed for devices that have keyboards or touch-screens emulating keyboards. Therefore, none of these methods can be applied in their original form on augmented-reality glasses, like the Google Glass, that do not support traditional user interfaces. Authentication methods that employ the novel interfaces of the Google Glass are yet to emerge. As mentioned before, the built-in mechanism is vulnerable to shoulder surfing attack. Some possible solutions for handling such an attack were outlined in [8]. The idea of voice command based PIN entry mechanism referenced in [8] is similar to the proposed VBP method. The system would display some random number for every digit and the user would have to add his secret digit to this random number and speak the result mod 10. Manual computation required to enter the PIN makes this method less usable. The other mentioned concept is to display a randomly assigned letter to each digit, and the user has to utter the associated letters corresponding to the PIN digits. However, the authors did not present any prototype design and user study to evaluate the methods. This motivated us to explore alternative authentication schemes for the Google Glass with an aim to increase the security of the built-in method while at least maintaining its current usability level.

3 Authentication Mechanisms

In this section, the authentication mechanisms for voice and touch interfaces are presented in detail.

3.1 Voice-based PIN (VBP) Authentication

The VBP mechanism uses voice to capture a PIN to unlock the Google Glass. In case the PIN is spoken directly, anyone around the user can hear and learn the secret value. One possible solution is to conceal the real PIN with a cipher text. The ciphers representing the digits could be another set of digits or alphabets (for e.g., $\{A, ..., Z\}$) or short words (for e.g., $\{`cat', ..., `dog'\}$). One initial study with different types of ciphers

shows that users preferred digits as the cipher in terms of usability and time taken to authenticate. Hence, in our design we map plain text digits to cipher text digits. Of course, the mapping from plain text to cipher text PIN has to change with every instance. For this, the private display visible only to the user can be used.

The Google Glass display is programmed to show a numeric touchpad-like grid, with each cell containing two different digits as shown in Figure 2 (b). The digits on the left in the cells (white ones) represent the real PIN digits found in a standard numeric touchpad. The second digit on the right side (red ones) of each cell shows the randomly mapped cipher digit that the user will have to utter in order to enter the corresponding real PIN digit. So for instance, in Figure 2(b), cipher digit 7 is used to represent PIN digit 1. To enter the PIN, the user is required to utter the red cipher digits which will then be mapped back to the actual cell numbers to compute the PIN. For instance to enter PIN 3961, a user has to utter 2437 (see Figure 2(b)).

The voice signal, captured by the mounted microphone on the Google Glass, is then processed by the Android speech recognition API to detect the corresponding cipher digits. Once the digits are recognized, the input PIN is computed by reverse mapping of the cipher digits into the corresponding real PIN numbers. If the detected input PIN matches with the stored PIN, the user is granted access to the Google Glass. It should be noted that the randomly assigned red cipher digits change with every instance.

3.2 Touch-based PIN (TBP) Authentication

The second authentication mechanism uses the mounted touchpad and requires swipe and tap gestures on the touchpad to enter the PIN. Since the Google Glass has the downward swipe reserved for the 'go back' or 'return to the Home screen' actions, the proposed method is designed with forward and backward swipes only. Figure 2(c) shows the layout of the user interface for the TBP mechanism. As can be observed from the figure, the cells of the virtual grid are overlaid with different digits which are randomly arranged for each authentication input.

To enter a PIN, the user is required to navigate to each of the corresponding cells using swipes and select the digit by tapping. Forward and backward swipe movements allow the user to move from the current cell to the next cell or previous cell, respectively. To verify a user, the input PIN is compared with the stored one. If they are matched, access is granted.

Since the digit assignment to the grid is different on every instance, the sequence of gestures performed by the user to enter the same PIN will be different each time. Hence, even by observing finger movements on the touchpad, it is difficult to deduce the actual PIN.

4 User Study

A user study was performed to systematically evaluate the properties of the VBP and TBP as alternate authentication mechanisms in terms of their security, usability, effectiveness (e.g., login success rate), efficiency (e.g., login times), and likeability. The study also investigated the following presumptions:

1. The login time for the PIN-based methods will decrease as the user becomes more familiar with the method.

2. The time it takes for authentication and the effort required are negatively correlated with preference.
3. One single mechanism of authentication is not enough for the different environments in which the Google Glass may be used. There is a need for multiple login mechanisms that can be efficiently used in specific situations. A voice based technique such as VBP might be preferred when the user's hands are busy, whereas the TBP might be suitable in noisy environments or situations where the user is not comfortable speaking the PIN loudly.

We used a Google Glass with 1.2 Ghz dual-core processor, 1 GB RAM, 16 GB memory, and display of 640×360 pixels for the study. The applications were developed on the Android platform 4.4. The user's identity was protected as no information about the user was stored that would make it possible to identify them.

4.1 Participants

The study was conducted with a total of 30 participants (11 females and 19 males) in a quiet conference room. The subject pool comprised high school, undergraduate, graduate, PhD students, and faculty without any security expertise. Among the users, only 16.67% had some prior experience with the Google Glass. 56.67% of the participants belonged to the 18-24 years age group, 23.33% to the 25-30 years group, 6.67% to the 30-35 years group, and the remaining 13.33% to the 35-40 years group.

75% of the users reported that they use a locking mechanism for their phone. 70% of the users strongly agreed that they would be concerned if someone gained access to their Google Glass assuming that the Glass contained or provided access to their personal information such as pictures, videos, messages, and emails. 72.4% of the users said that they would like to use a locking mechanism for the Glass and that they believe it is important to have it in order to protect their private information.

4.2 User Study Design

The passwords were fixed in advance to limit the number of variables affecting the experiment and to ensure that sufficiently complex passwords were used. Two sets of passwords were chosen as mentioned below:

- Set 1 : PIN was 8340. Pattern was two-finger swipe forward, tap, hook swipe forward, two-finger swipe back.
- Set 2 : PIN was 2791. Pattern was two-finger swipe back, swipe forward, two-finger tap, hook swipe forward.

The PINs were chosen with no repeated, consecutive or neighboring digits. The same PIN was used for the VBP and TBP mechanisms to allow for comparison between the methods. Similarly, for the built-in mechanism, patterns of high strength were chosen. The use of two sets of passwords helped in minimizing the effect of password choice on the analysis.

The group of 30 users was randomly divided into two subgroups and each subgroup was assigned with one of the password sets. Each participant performed three authentication methods in random order to ensure no bias towards a particular mechanism. After an introductory session, each user went through three authentication sessions and a final feedback session as described below.

Introductory Session (5 min): The user was given a short tutorial on how to handle the Google Glass and was allowed to operate and get familiarized with the Glass. The user was assigned the passwords according to the group he/she belonged to.

Authentication Session (approximately 60 min): For each authentication mechanism, the users went through three phases: (1) practice (2) verification, and (3) survey.

At the beginning of each experimental condition, the authentication method was first briefly explained and the user was guided through the authentication interface. The user was allowed to practice the authentication method for a brief time.

Following the practice phase, the user was asked to log into the Google Glass repeatedly until ten successful logins were achieved. The user's inputs, authentication times, and authentication success rates were recorded during this verification phase.

Finally, the user answered a number of questions about usability and security of the authentication mechanism just used before moving on to the next mechanism.

Feedback Session (5 min): At the end of the study, the users were asked a final set of questions comparing all the methods.

4.3 Questionnaire

Part I: At the end of each authentication session, participants were asked to evaluate the security and usability of the method. To get subjective assessment about the usability, the ten-question System Usability Scale (SUS) [27] was used. The term "system" in SUS refers to the "authentication method" to be evaluated in our study. In the SUS assessment, responses to each of the ten questions are given on a five-point scale ranging from "strongly disagree" to "strongly agree". Apart from the raw SUS score, for better interpretation of the results, SUS percentile [28] and corresponding A-F grading [29] are also reported in this paper.

Part II: Next, five questions were asked about perceived security, convenience, speed, stability, and PIN guessability using the same five-point response scale as follows: (a) I think the method is very secure, (b) I think the method is very convenient, (c) I think the method is very fast, (d) I think the method is very stable, (e) I think the degree of guessability of the PIN is high using this method.

Part III: At the end of the experiment, the users were asked to rank the methods in terms of security, login time, comfort, and likelihood of future use. Some of the questions from Part II were repeated here to study whether the user's perception changes after using all the methods.

Part IV: To get insight about the preference of the users in choosing different mechanisms in different usage situations of the Google Glass, the users were asked to rank the methods based on the likelihood of future usage in the following situations: (a) a quiet classroom or office, (b) a busy subway or a party, (c) at home with family or friends, (d) at home alone, (e) during jogging or biking, (f) listening to loud music alone.

5 Results

This section summarizes the results obtained by the study as described above.

5.1 Login Success Rate

For the VBP, 13% of the participants accomplished the criterion of 10 successful logins in 10 attempts with no incorrect logins, 63% participants made 1-3 incorrect logins and the rest required more than 3 attempts making the mean percentage of accuracy for password inputs to be 83% as shown in Table 1. The reason behind failure to authenticate was one of the following: (a) wrong user input (b) client side error and no speech input due to weak internet connection or heating up of the Google Glass for prolonged use and (c) incomplete voice signal as the user took more time than the allocated one (20s). It was observed that the utterance of wrong sequence of digits caused error only 32.4% times while the other two reasons happened 58.1% and 9.5% times, respectively.

Table 1. Performance study

	VBP	TBP	Built-in Method
Average Success Rate (%)	83	87	68
Average Authentication Time (Secs)	6.4	13.9	5.6

For the TBP, 27% of the users logged in without any error, 57% accomplished it with maximum 3 incorrect attempts. The overall success rate was 87%.

For the built-in method, the success rate was lowest, i.e., 68%. Only 7% of the users were able to login in the first attempt and 17% made 1-3 incorrect logins. Most of the users required more than 13 attempts to perform 10 correct logins. Since all the computations were done on the Google Glass itself without information being sent over the network to external server, the only reason behind failure to authenticate for both the TBP and built-in techniques was wrong user input.

5.2 Authentication Time

The authentication time was calculated from the time a participant starts entering the password to the time that he/she successfully logs into the device. It includes the time spent to enter the VBP or TBP (for the built-in method, this is the time to enter the pattern), processing time to perform authentication, and server response delays.

This measure was calculated for the 10 successful trials per participant. Table 1 shows the average time taken by each successful trial for the three authentication mechanisms. It can be observed from these comparisons that the VBP mechanism approximately takes the same authentication time as the built-in method, while the TBP method takes much longer.

The variation in authentication time with 10 login attempts is shown in Figure 3. The time required for a successful login decreases with successive runs as the users become more skillful and comfortable with the mechanism. The median authentication time also indicates a slight learning curve. The learning effect on the speed of authentication is shown in Figure 4.

5.3 Usability and Security Study

As described in Section 4.3 Part I questionnaire, users were asked 10 SUS questions about the respective method. It has been observed from the feedback that participants

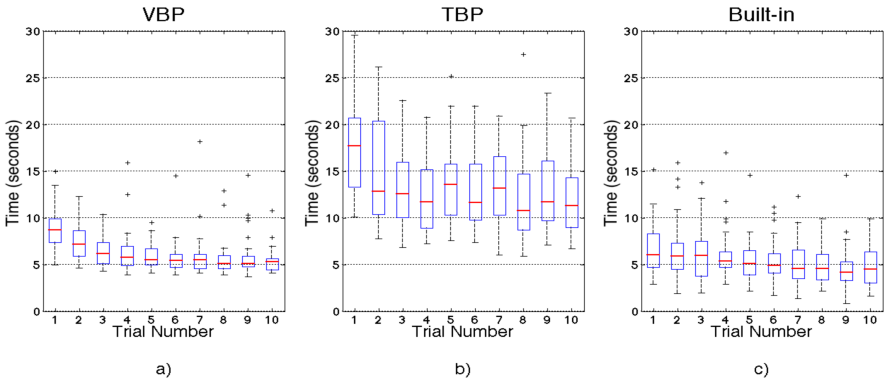

Fig. 3. Variations in login time for 10 trials using (a) VBP (b) TBP (c) built-in method

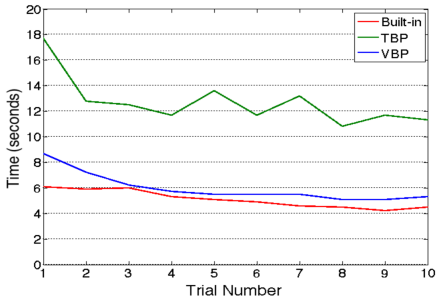

Fig. 4. Variations in median login time over 10 trials using the VBP, TBP and built-in method

rated the VBP high as compared to the other two methods on the usability factors, such as "ease of use" (question 3 of SUS), "would like to use" (question 1 of SUS). Most of them also reported that the VBP could be learned quickly (question 7 of SUS) without taking any technical help (question 4 of SUS) as it was less complex (question 2 of SUS), less cumbersome (question 8 of SUS), and well integrated (question 5 of SUS) compared to the TBP and built-in methods. Users perceived the built-in method to be more complex and hence could not be learned as easily as the two PIN-based methods. Moreover, the built-in method is more inconsistent (question 6 of SUS) and the users had lowest confidence (question 9 of SUS) using the method.

Table 2. System Usability Scale (SUS) study

	VBP	TBP	Built-in Method
SUS Score	76.1%	69.1%	61.2%
SUS Response Percentile (approx.)	77th	54th	33th
SUS Grade	B	C	C

Results of quantitative analysis of the feedback are reported in Table 2. The table shows the average SUS score, response percentile, and grade for each authentication mechanism. The VBP was rated highest with a score of 76.1%, well above the average SUS response value (68%). This marks the VBP in the 77th percentile with a SUS grade of B. The TBP method also scored above the average SUS response value, with score of

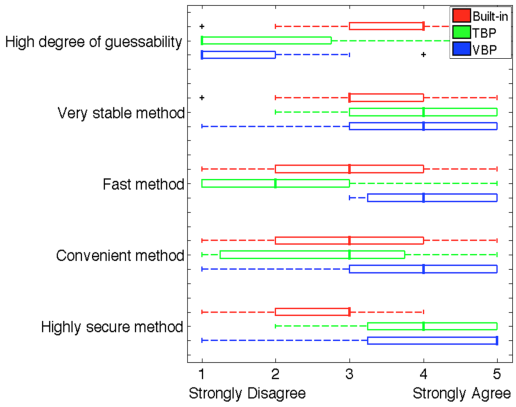

Fig. 5. Overall user experience after using the VBP, TBP, and built-in method

69.1%, 54th percentile and a SUS grade of C. The built-in mechanism was rated lowest, with a SUS score of 61.2%, 33th percentile and a SUS score of C.

Figure 5 shows the result of Part II questionnaire in Box plot using the same 5-point Likert scale (in the 5 point scale 1 represents "strongly disagree" and 5 represents "strongly agree"). Based on this feedback, the average score for each method is computed as shown in Table 3.

Table 3. Overall user experience results

	VBP	TBP	Built-in method
Security	4.17	4.14	2.50
Convenience	3.53	2.57	3.10
Speed	4.20	2.33	2.90
Stability	3.53	3.90	3.20
Degree of Guessability	1.93	2.07	3.53

It can be observed from the median ratings in Figure 5 that the security of the VBP and TBP was thought to be higher than the built-in method. VBP was perceived as most secure with an average score of 4.17 out of 5. Average score for the TBP is 4.14, which is comparable to the VBP. The VBP was also considered to have the lowest degree of PIN guessability with a score of 1.93. The average score of the TBP (2.07) is also significantly lower than that of the built-in method (3.53).

In terms of convenience, the VBP was rated highest with an average score of 3.53 out of 5, followed by the built-in method and TBP.

The users perceived the VBP to be the fastest one (average score 4.20 out of 5) and the TBP to be slowest (average score 2.33 out of 5). This ranking contradicts with the ranking based on actual average authentication time reported in Table 1, where the built-in method required least time. The perceived speed for the TBP (2.33 in 5) was also close to the built-in method (2.90 in 5). This observation shows that although the VBP or TBP required more processing time, they were not perceived as onerous.

The users also reported that the two PIN-based mechanisms were more stable than the built-in method. The TBP was rated as the most stable method with a score of 3.90.

5.4 Overall User Experience

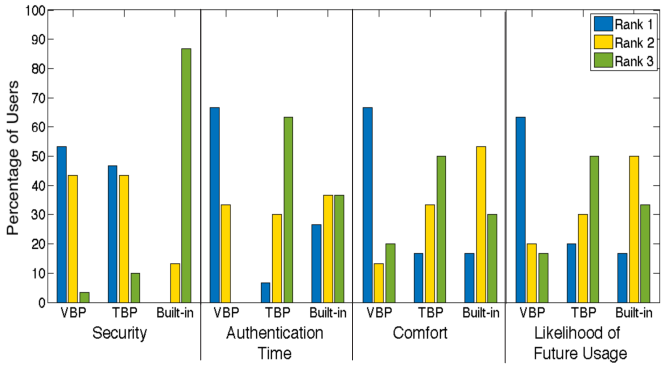

Fig. 6. User rankings of the VBP, TBP, and built-in method in terms of security, authentication time, comfort, and likelihood of future usage

The feedback data for Part III questionnaire is plotted in Figure 6.

For security, 53.3% of the users ranked the VBP first and 46.7% ranked the TBP first. This result goes along with the feedback taken after each authentication session (discussed in the previous section), which shows that VBP was perceived to be the most secure authentication method.

In terms of authentication time, 66.7% of the users ranked the VBP first whereas 26.7% ranked the built-in method first. This feedback also supports our previous observation that VBP's perceived speed is higher than that of the built-in method in spite of having longer login time.

In the case of comfort, the VBP was ranked first by 66.7% of the users, whereas the other methods got 16.7% of the votes each. Similarly, 63.3% of the users gave first rank to the VBP for the likelihood of future usage, 20.0% for the TBP, and 16.7% for the built-in mechanism. This shows that the users had a clear inclination towards the PIN-based techniques over the built-in method.

5.5 Context Dependent Preference Study

Figure 7 shows the feedback of the users for Part IV questionnaire.

For the first situation, a quiet office or classroom, 43.3% of the users ranked the TBP as first and 36.7% ranked the built-in method as first. Similarly, for the second situation, a busy subway or social gathering, 56.7% of the users ranked the TBP as first and 30% ranked the built-in method as first. In spite of being slower, users preferred the TBP more than the built-in method in public settings. This shows users' concern about the low security of the built-in method. They were ready to compromise on speed to ensure enhanced security.

For the third situation, at home with family or friends, the VBP was ranked first by 53.3% of the users, whereas the other methods got only 23.3% of the votes each.

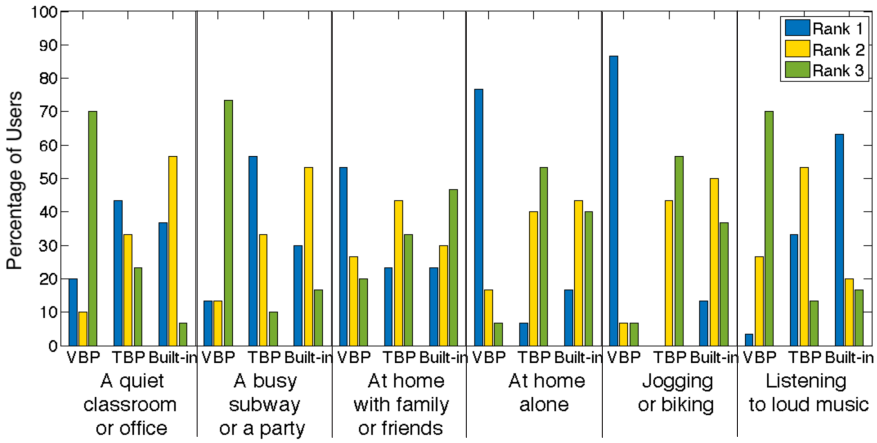

Fig. 7. User rankings of the VBP, TBP, and built-in method in different usage scenarios

For the fourth situation, at home alone, 76.7% of the users ranked the VBP as first and only 16.7% ranked the built-in method as first. For the fifth situation, while jogging or biking, 86.7% ranked the VBP as first. Thus, whenever users had a chance to use the VBP (in low background noise situation), they always chose it over any other method.

For the sixth situation, listening to loud music alone, 63.3% ranked the built-in method as first and 33.3% ranked the TBP as first. Since the users would be alone, there was less concern about security. Hence, they felt comfortable to use the built-in method in place of the TBP.

The above study shows that while choosing one mechanism, security is the most important criterion to the users. As a consequence, PIN-based mechanisms were preferred in all the public settings. Even if the users were alone, they opted for the VBP if viable. Only in the last case, the built-in method was chosen as security was not a concern and the VBP could not be used.

6 Discussion

Effectiveness: The study provides an understanding of the relative user effort required by the different authentication techniques. With minimal instructions and very little practice, the users were able to login using the TBP and VBP successfully more than 80% of the time whereas using the built-in mechanism they succeeded only 68% of the time. This shows that the PIN-based mechanisms are more effective than the built-in one. Moreover, incase of VBP, authentication failure due to incorrect user input accounted for only 32.4% of all the failed authentication attempts and the rest were due to limitations at the level of Google Glass. With this observation, it is safe to say that VBP will be much more effective with the advancements in the Glass technology.

Efficiency: While the VBP and built-in methods had comparable login times, the TBP needed a significantly longer login time. Multiple horizontal swipes needed to select the desired digits of the PIN may lead to longer login time. On an average, the VBP and built-in method had an 8.0-8.4s shorter login time than the TBP.

However, the actual authentication time does not always match with the users' perception of speed of an authentication mechanism. Although the built-in method outper-

formed the TBP and VBP in terms of authentication time, participants rated VBP as the fastest. Further, the TBP scored quite close to the built-in mechanism in spite of taking almost double average login time. The effort required to enter a PIN may have affected users' perception of speed.

Learning Effect: One way the PIN input can be speeded up is for users to become more skillful. In our study, all the participants were novice users who were able to increase their speed moderately in the VBP and built-in mechanism over ten trials. However, significant improvement in speed with the TBP was observed, where average login time was halved in 10^{th} trial from the 1^{st} one. This gives us reason to hope that with practice the TBP would be more efficient and acceptable. Thus, the first presumption mentioned in Section 4 is validated. Further field studies in natural environments with more experienced users are needed to get a more complete understanding of the learning effect.

Usability: User responses to the SUS were above average for the two PIN-based authentication mechanisms. The built-in mechanism scored lower than average, which indicates that it was not well accepted by the users in spite of being faster. Overall, users were more satisfied with the new mechanisms compared to the built-in one. This observation was supported by the outcome of the feedback question on likelihood of future usage at the end of the experiment, where participants rated the VBP first followed by the TBP and built-in mechanisms.

Discussion on login time, perceived speed, and likelihood of future usage shows that users always preferred the method with least effort, i.e., VBP. This may not lead to choosing the method with least authentication time. Perceived speed played a more important role in the selection. Thus, our second presumption is partially confirmed.

Security: With respect to security, participants always rated the VBP and TBP much higher than the built-in method. They also reported that the guessability of the PIN using the built-in method is much higher than the two proposed mechanisms. Inclination towards the VBP and TBP was also evident from the users' choice of authentication technique in public space. They always opted for either one of these two methods over the built-in one.

Preferred Mechanism in Hypothetical Usage Situations: Feedback on the likelihood of usage of the three authentication techniques in different usage contexts shows that people tend to choose different authentication mechanisms depending on the environment. Apart from the situational constraints, security was an important aspect in selecting the method. The built-in mechanism was never chosen in public settings.

To choose the preferred authentication method, just like the main menu of the Google Glass, user needs to simply utter 'yes' or 'no' for an authentication option seen on the screen or tap to choose an option. This would allow for a successful integration of the two methods in a real system, without significantly increasing authentication time.

Limitations: The main drawback of the proposed method is that it restricts the use of PINs with repeated digits. The problem is more prominent with VBP, whereas TBP suffers only if there is consecutive occurrences of same digit. Even if a single digit of a PIN is repeated, then the number of guessable passwords reduces to 1000. However, the problem can be solved by changing the cipher digit assignment or the keypad layout after each digit entry for VBP and TBP, respectively.

7 Conclusions

This paper presents two PIN based authentication methods, namely, TBP and VBP for the Google Glass. Both of them take advantage of the unique characteristics of the wearable device, especially the private display, to make the method robust against shoulder surfing and eavesdropping. Since the same PIN can be entered using both methods, a user has the freedom to choose any one depending on the environment.

A detailed user study was conducted to compare the PIN based authentication techniques with the built-in method, testing authentication accuracy, security, usability and overall user experience. The results show that VBP and TBP have better accuracy than the built-in method, users being able to successfully login more than 80% of the time using the VBP or TVP, while only 68% of the time using the built-in mechanism. The VBP and built-in methods have comparable login times ($\sim$8s) but the TBP requires a significantly longer login time (14s). However, users perceived VBP to be the fastest followed by the built-in and TBP methods. In terms of perceived security, the VBP and TBP were ranked ahead of the built-in method. 53.3% of the users ranked the VBP and 46.7% ranked the TBP as the most secure mechanism. The usability of the PIN based methods was also higher as the SUS score for the VBP (76.1%) and TBP (69.1%) was better than that for the built-in method (61.2%). The results also suggest that the PIN based authentication mechanisms have overall better user perception in terms of stability, and likeability than the built-in method. Further, the study provides insight into users' preference when using these three techniques under different contexts. The PIN based techniques complement one another in different scenarios and were preferred more in public settings than the built-in one. The results show that the PIN based methods have the potential to be used for secure user authentication on Google Glass in various usage contexts.

Acknowledgment

This work is supported by the National Science Foundation under Grant No. 1228842.

References

1. Google Glass. http://www.google.com/glass/start/
2. Glauser, W.: Doctors among early adopters of Google Glass. Canadian Medical Association Journal. cmaj-109 (2013).
3. McNaney, R., Vines, J., Roggen, D., Balaam, M., Zhang, P., Poliakov, I., Olivier, P.: Exploring the acceptability of google glass as an everyday assistive device for people with parkinson's. Proc. of CHI, 2551-2554 (2014).
4. Hernandez, J., Li, Y., Rehg, J. M., Picard, R. W.: BioGlass: physiological parameter estimation using a head-mounted wearable device. Accepted in Mobihealth.
5. Ishimaru, S., Kunze, K., Kise, K., Weppner, J., Dengel, A., Lukowicz, P., Bulling, A.: In the blink of an eye: combining head motion and eye blink frequency for activity recognition with Google Glass. Proc. of the Augmented Human Int'l Conf., 15 (2014).
6. Yus, R., Pappachan, P., Das, P. K., Mena, E., Joshi, A., Finin, T.: Demo: FaceBlock: privacy-aware pictures for google glass. Proc. of Int'l Conf. on Mobile Systems, Applications, and Services, 366 (2014).

7. Egelman, S., Jain, S., Portnoff, R. S., Liao, K., Consolvo, S., Wagner, D.: Are you ready to lock? understanding user motivations for smartphone locking behaviors. Proc. of ACM SIGSAC Conf. on Computer and Communications Security, (2014).
8. Bailey, D. V., Drmuth, M., Paar, C.: Typing passwords with voice recognition: How to authenticate to Google Glass. Proc. of the Symposium on Usable Privacy and Security , (2014).
9. Rogers, J. Please enter your four-digit pin. Financial Services Technology, U.S. Edition, 4 (2007).
10. Ratha, N. K., Chikkerur, S., Connell, J. H., Bolle, R. M.: Generating cancelable fingerprint templates. IEEE Trans. on PAMI, 29(4), 561–572, (2007).
11. Weiss, R., De Luca, A.: PassShapes: utilizing stroke based authentication to increase password memorability. Proc. of NordiCHI, 383-392 (2008).
12. Davis, D., Monrose, F., Reiter, M. K.: On user choice in graphical password schemes. Proc. of USENIX Security Symposium, 13, 1–14 (2004).
13. Birget, J.-C., Dawei H, Memon, N.: Graphical passwords based on robust discretization. IEEE Trans. on Information Forensics and Security, 1(3), 395–399 (2006).
14. Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., Rubin, A. D.: The design and analysis of graphical passwords. Proc. of SSYM, (1999).
15. Dirik, A. E., Memon, N., Birget, J. C.: Modeling user choice in the PassPoints graphical password scheme. Proc. of Usable Privacy and Security, 20–28 (2007).
16. http://www.passfaces.com/pfphelp/logon.htm.
17. Roth, V., Richter, K., Freidinger, R.: A pin-entry method resilient against shoulder surfing. Proc. of Conf. on Computer and Communications Security, 236245 (2004).
18. Wiedenbeck, S., Waters, J., Sobrado, L., Birget, J.-C.: Design and evaluation of a shoulder-surfing resistant graphical password scheme. Proc. of Conf. on Advanced Visual Interfaces, 177184 (2006).
19. Bianchi, A., Oakley, I., Kwon, D. S.: The secure haptic keypad: a tactile password system. Proc. of Int'l Conf. on Human Factors in Computing Systems, 10891092 (2010).
20. Kim, D., Dunphy, P., Briggs, P., Hook, J., Nicholson, J., Nicholson, J., Olivier, P.: Multitouch authentication on tabletops. Proc. of Int'l Conf. on Human Factors in Computing Systems, 10931102 (2010).
21. De Luca, A., von Zezschwitz, E., Hussmann, H.: Vibrapass: secure authentication based on shared lies. Proc. of Int'l Conf. on Human Factors in Computing Systems, 913916 (2009).
22. De Luca, A., Hang, A., Brudy, F., Lindner, C., Hussmann, H.: Touch me once and I know its you! Implicit authentication based on touch screen patterns. Proc. of Int'l Conf. on Human Factors in Computing Systems, (2012).
23. Sae-Bae, N. Memon, N.: Online signature verification on mobile devices. IEEE Trans. on Information Forensics and Security, 9(6), 933947 (2014).
24. Sae-Bae, N., Memon, N., Isbister, K. Ahmed, K.: Multitouch gesture-based authentication. IEEE Trans. on Information Forensics and Security, 9(4), 568 582 (2014).
25. Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S., Glezer, C.: Google android: A comprehensive security assessment. Security Privacy IEEE, 8(2), 35 44 (2010).
26. Von Zezschwitz, E., Dunphy, P., De Luca, A.: Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices. Proc. of Int'l Conf. on Human-computer Interaction with Mobile Devices and Services, 261-270 (2013).
27. Brooke, J.: SUS: A quick and dirty usability scale. Taylor and Francis, 189194 (1996).
28. Sauro, J.: Measuring usability with the System Usability Scale (SUS), (2011).
29. Bangor, A., Kortum, P. T., Miller, J. T.: An empirical evaluation of the system usability scale. Int'l Journal of Human-Computer Interaction, 24(6), 574-594 (2008).