Reducing Shoulder-surfing by Using Gaze-based Password Entry

Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd
Stanford University
Gates Building
353 Serra Mall, Stanford, CA
+1.650.725.3722
{sneaker, talg, dabo, winograd}@cs.stanford.edu

ABSTRACT

Shoulder-surfing – using direct observation techniques, such as looking over someone's shoulder, to get passwords, PINs and other sensitive personal information – is a problem that has been difficult to overcome. When a user enters information using a keyboard, mouse, touch screen or any traditional input device, a malicious observer may be able to acquire the user's password credentials. We present EyePassword, a system that mitigates the issues of shoulder surfing via a novel approach to user input.

With EyePassword, a user enters sensitive input (password, PIN, etc.) by selecting from an on-screen keyboard using only the orientation of their pupils (i.e. the position of their gaze on screen), making eavesdropping by a malicious observer largely impractical. We present a number of design choices and discuss their effect on usability and security. We conducted user studies to evaluate the speed, accuracy and user acceptance of our approach. Our results demonstrate that gaze-based password entry requires marginal additional time over using a keyboard, error rates are similar to those of using a keyboard and subjects preferred the gaze-based password entry approach over traditional methods.

Categories and Subject Descriptors

K.6.5 [**Security and Protection**]: Authentication. H.5.2 [**User Interfaces**]: Input devices and strategies.

General Terms

Security, Human Factors

Keywords

Shoulder surfing, password entry, eye tracking, gaze-based password entry.

1. INTRODUCTION

Passwords remain the dominant means of authentication in today's systems because of their simplicity, legacy deployment and ease of revocation. Unfortunately, common approaches to entering passwords by way of keyboard, mouse, touch screen or any traditional input device, are frequently vulnerable to attacks such as shoulder surfing and password snooping.

Current approaches to reducing shoulder surfing typically also reduce the usability of the system; often requiring users to use security tokens [32], interact with systems that do not provide direct feedback [31, 40] or they require additional steps to prevent an observer from easily disambiguating the input to determine the password/PIN [5, 12, 31, 36, 39, 40]. Previous gaze-based authentication methods [16, 17, 23] do not support traditional password schemes.

We present EyePassword, an alternative approach to password entry that retains the ease of use of traditional passwords, while mitigating shoulder-surfing and acoustics attacks. EyePassword utilizes gaze-based typing, a technique originally developed for disabled users (like [4]) as an alternative to normal keyboard and mouse input. Gaze tracking works by using computer vision techniques to track the orientation of the user's pupil to calculate the position of the user's gaze on the screen.

Gaze-based password entry makes gleaning password information difficult for the unaided observer while retaining the simplicity and ease of use for the user. As expected, a number of design choices affect the security and usability of our system. We discuss these in Section 3 along with the choices we made in the design of EyePassword. We implemented EyePassword using the Tobii 1750 [38] eye tracker and conducted user studies to evaluate the speed, accuracy and user acceptance. Our results demonstrate that gaze-based password entry requires marginal additional time over using a keyboard, error rates are similar to those of using a keyboard and users indicated that they would prefer to use the gaze-based approach when entering their password in a public place.

2. BACKGROUND AND RELATED WORK

Shoulder-surfing is an attack on password authentication that has traditionally been hard to defeat. It can be done remotely using binoculars and cameras, using keyboard acoustics [9, 10, 42], or electromagnetic emanations from displays [19]. Access to the user's password simply by observing the user while he or she is entering a password undermines all the effort put in to encrypting passwords and protocols for authenticating the user securely. To some extent, the human actions when inputting the password are the weakest link in the chain.

Biometric methods, which identify individuals based on physiological or behavioral characteristics, have the advantage that they are harder to replicate and therefore are not susceptible to the risks of shoulder surfing. However, biometric techniques

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.

Symposium On Usable Privacy and Security (SOUPS) 2007, July 18-20, 2007, Pittsburgh, PA, USA.

suffer from the drawback that biometric characteristics are non-secret and non-revocable. While it is easy for a user to change a password, it is a considerably less convenient and presumably more painful procedure for the user to change a fingerprint or retinal scan.

Physical token based approaches such as the RSA SecurID token [32] overcome shoulder-surfing, but such devices require users to carry a physical access token, which is prone to being lost or stolen. The Scramble Keypad Reader [6] uses a 7-segment LED display inside each keypad pushbutton. The location of the digits on the keypad is randomized with each trial thereby reducing the risk of shoulder surfing. This keypad also uses two pieces of metal on either side of the keypad to prevent other people from seeing the keys being pressed.

In general, approaches to overcoming shoulder surfing rely on "increasing the noise" for the observer so that it becomes difficult for the observer to disambiguate the user's actions/input. Roth et al [31] present an approach for PIN entry which uses the philosophy of increasing the noise for the observer. In their approach, the PIN digits are displayed in two distinct sets colored black and white. For each digit the user must make a series of binary choices as to which set (black or white) the PIN digit appears in. The correct PIN digit is identified by intersecting the user's set choices. The approach requires users to make multiple binary selections in order to correctly input each digit of the PIN.

Wiedenbeck et al [40] introduce a shoulder-surfing-resistant graphical password scheme. The user selects a number of icons as his or her pass icons. When logging in, the user is presented with a random assortment of icons. The user must find the pass icons previously identified, create a mental image of the convex hull formed by these icons and then click inside this convex hull. The scheme again relies on multiple challenge response passes in order to successfully authenticate the user. This approach requires the user to learn a new approach and also increases the length of the authentication process.

PassFaces [5] relies on the user recognizing faces and pointing to recognized faces as responses to a series of challenges. Hoanca et al [17] extend PassFaces using eye gaze for selecting the face from within the grid. Weinshall [39] introduces an approach that uses a set of machine generated pictures as the user's password. The user must memorize the pictures. When presented with the login screen, the user must mentally trace a path which includes the password pictures and answer a multiple choice question. A series of challenge-response sets result in authentication. Since only the user knows which path was traced, a human or software observer (spy-ware) would be unable to determine the correct password. However, as the author states, "the benefit is obtained at the cost of a relatively long login time of a few minutes." The approach has been shown to be insecure against an eavesdropping adversary in [12].

Tan et al [36] propose a spy-resistant keyboard, which uses a level of indirection to prevent the observer from guessing the password. Their approach adds sufficient ambiguity for the observer to be unable to determine the user's choice without remembering the layout of the entire keyboard. However, to enter the password, users must use an unfamiliar keyboard layout and complex interaction technique.

While there are other approaches to prevent shoulder surfing [16], it is sufficient to note that all the approaches have the common theme of increasing the noise/ambiguity for the observer. Usually this is achieved by increasing the number of interactions the user must do to successfully log in.

Maeder et al [23] present a gaze-based user authentication scheme in which a user is presented with an image and must dwell upon previously specified points of interest on the image in a predetermined order in order to log in. The authors do not present an analysis of the ease with which a malicious user may guess the order of the points of interest on the image. In addition, this scheme doesn't support the use of traditional passwords.

Other approaches to overcoming shoulder-surfing include the use of tactile passwords [33] or more invasive techniques such as brain computer interfaces [37].

Gaze-based typing has been extensively researched [14, 24-26] and is used by several commercial systems [2, 4]. The primary difference between using gaze for typing and for password entry is how feedback is managed. Thorpe et al [37] introduced the concept of using gaze-based password entry in their paper on Pass-thoughts. The authors noted that *"an eye-gaze based method could permit unobservable passwords of the same strength provided by textual or graphical password schemes by allowing the user to select parts of the password with their eyes (e.g. by eye fixation for a specified period denoting selection), and not echoing the input on the screen."* In our work, we implemented the concept described above and conducted usability studies to evaluate the efficacy of gaze-based password entry.

3. MOTIVATION FOR EYE TRACKING

Eye tracking technology has come a long way since its origins in the early 1900's [18]. State of the art eye trackers offer non-encumbering, remote video-based eye tracking with an accuracy of 1° of visual angle. Eye trackers are a specialized application of computer vision. A camera is used to monitor the user's eyes. One or more infrared light sources illuminate the user's face and produce a glint – a reflection of the light source on the cornea. As the user looks in different directions the pupil moves but the location of the glint on the cornea remains fixed. The relative motion and position of the center of the pupil and the glint is used to estimate the gaze vector, which is then mapped to coordinates on the screen plane.

Commercial eye-trackers are currently very expensive, varying in price from US $5,000 to US $40,000. However, the underlying technology is straightforward [7, 8, 11, 15, 28-30, 41] and other than recovering the cost of research and development, there is no reason why an eye tracker should be so expensive. Technology and research trends [3, 8, 13, 21] indicate that the cost of eye-tracking systems should decline rapidly in the near future, making eye tracking a viable form of augmented input for computer systems.

Devices such as Apple's MacBook laptops include a built-in iSight camera [1] and hardware trends indicate that even higher resolution cameras will be embedded in standard display devices in the future. Using such a camera for eye tracking would only require the addition of inexpensive IR illumination and image processing software.

ATMs are equipped with security cameras and the user stands directly in front of the machine. Since ATM pins typically use only numbers, which need fewer distinct regions on the screen,

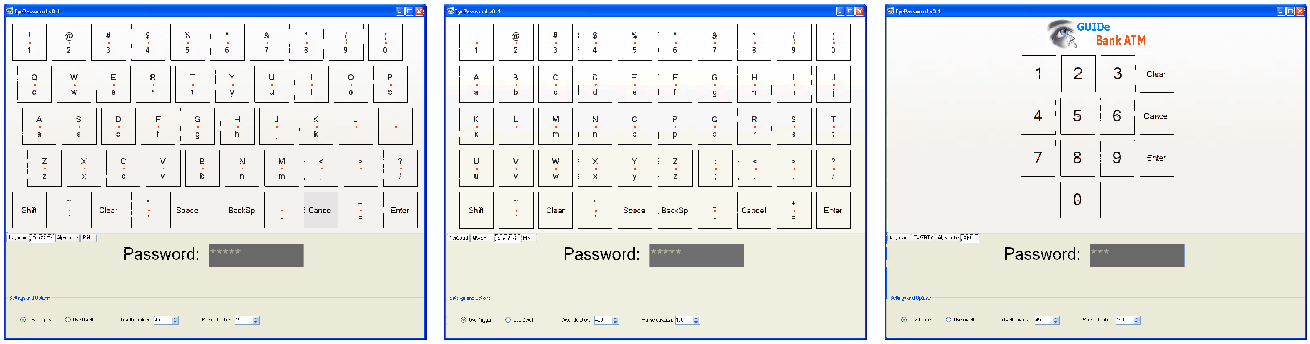

Figure 1. On-screen keyboard layout for gaze-based password entry showing QWERTY, Alphabetic and Keypad layout.

the quality of the eye tracking required for tracking gaze on an ATM keypad does not need to be as high as the current state-of-the-art eye trackers. Current generation eye trackers require a one-time calibration for each user. We envision a system where the calibration for each user can be stored on the system. Inserting the ATM card identifies the user and the stored calibration can be automatically loaded.

Gaze-based password entry has the advantage of retaining the simplicity of using a traditional password scheme. Users do not need to learn new way of entering their password as commonly required in the techniques described in the previous section. At the same time, gaze-based password entry makes detecting the user's password by shoulder surfing a considerably harder task, thereby increasing the security of the password at the weakest link in the chain – the point of entry. Gaze-based password entry can therefore provide a pragmatic approach achieving a balance between usability and security.

4. THREAT MODEL

We model a shoulder surfer as an adversary who observes the user's keyboard and screen. Moreover, the adversary can listen to any sound emanating from the system. Our goal is to build an easy to use password-entry system secure against such adversaries. We assume the adversary can observe the user's head motion, but cannot directly look into the user's pupils. A shoulder surfer looking at the user's eyes during password entry will surely arouse suspicion. We note that a video camera trained at both the computer screen and the user's eyes during password entry (essentially a homemade eye tracker) could defeat our system. The purpose of our system is to propose a pragmatic interaction which eliminates the vast majority of the shoulder-surfing attacks. It would indeed be difficult for a shoulder surfer to record both the screen activity and a high resolution image of the user's eyes and be able to cross-reference the two streams to determine the user's password.

5. DESIGN CHOICES

The basic procedure for gaze-based password entry is similar to normal password entry, except that in place of typing a key or touching the screen, the user looks at each desired character or trigger region in sequence (same as eye typing). The approach can therefore be used both with character-based passwords by using an on-screen keyboard and with graphical password schemes as surveyed in [35]. A variety of considerations are important for ensuring usability and security.

5.1 Target Size

The size of the targets on the on-screen keyboard should be chosen to minimize false activations. The key factor in determining the size of the targets is not the resolution of the display, but the accuracy of the eye tracker. Since the accuracy is defined in terms of degrees of visual angle, the target size is determined by calculating the spread of the angle measured in pixels on the screen at a normal viewing distance.

The vertical and horizontal spread of the 1 degree of visual angle on the screen (1280x1024 pixels at 96 dpi) at a normal viewing distance of 50 cm is 33 pixels. This implies that when looking at a single pixel sized point, the output from the eye-tracker can have a uncertainty radius of 33 pixels, or a spread of 66 pixels. The size of the targets should be sufficiently greater than 66 pixels to prevent false activations. We chose a target size of 84 pixels with a 12 pixel inter-target spacing to minimize the chances of false activations when using gaze-based selection.

While it is certainly possible to use gaze-based password entry with eye movements alone and no corresponding head movements, we observed that subjects may move their head when looking at different parts of the screen. Though the head movements are subtle they have the potential to reveal information about what the user may have been looking at. For example, the attacker may deduce that the user is looking at the upper right quadrant. Clearly, the smaller and more tightly spaced the keys in the on-screen keyboard, the less information the attacker obtains from these weak observations. This suggests a general design principle: the on-screen keyboard should display the smallest possible keys that support low input error rates.

5.2 Keyboard Layout

Since muscle memory from typing does not translate to on-screen keyboard layouts, the user's visual memory for the spatial location of the keys becomes a more dominant factor in the design of on-screen keyboards. The trade-off here is between usability and security - it is possible to design random keyboard layouts that change after every login attempt. These would require considerably more visual search by the user when entering the passwords and therefore be a detriment to the user experience, but would provide increased security. We chose not to use randomized layouts in our implementation.

5.3 Trigger Mechanism

There are two methods for activating character selection. In the first method, dwell-based [24] the users fix their gaze for a

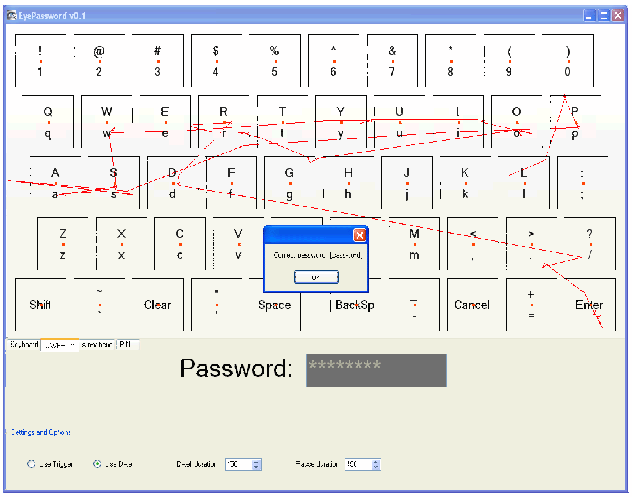

Figure 2. Gaze-pattern when the user enters "password" as the password. Each key has a bright red dot at the center of it. This *focus point* allows the user to focus their gaze at the center of the target thereby increasing the accuracy of eye tracking data.

character and then presses a dedicated trigger key such as the spacebar. Using a dedicated trigger key has the potential to reveal timing information between consecutive character selections, which can enable an adversary to mount a dictionary attack on the user's password [34]. The dwell-based method hides this timing information. Furthermore, our user studies show that dwell-based methods have lower error rates than the multi-modal methods.

5.4 Feedback

Contrary to gaze-based typing techniques [25], gaze-based password entry technique should not provide any identifying visual feedback to the user (i.e. the key the user looked at should not be highlighted). However, it is still necessary to provide the user with appropriate feedback that a key press has indeed been registered. This can be done by sounding an audio beep or flashing the background of the screen to signal the activation. Additional visual feedback may be incorporated in the form of a password field that shows one additional asterisk for each character of the password as it is registered. To reduce the amount of timing information leaked by the feedback mechanism, the system can output a feedback event only in multiples of 100ms. In either case, the feedback will leak information regarding the *length* of the password.

5.5 Shifted Characters

Limits on screen space may prevent all valid password characters (e.g., both lower and upper case) from being displayed in an on-screen layout. Our implementation shows both the standard character and the shifted character in the same target. To type a shifted character, the user activates the shift key once, which causes the following character to be shifted. This approach reveals no additional information to the observer. An alternative approach would be to show only the standard character on-screen and change the display to show the shifted characters once the user activates the shift mode. However, this approach would leak additional information to the observer about the user's password.

6. IMPLEMENTATION

We implemented EyePassword on Windows using a Tobii 1750 eye tracker [38] set to a resolution of 1280x1024 pixels at 96 dpi. Figures 1 shows the EyePassword on-screen keyboards using a QWERTY, alphabetic and ATM pin keypad layout respectively. To reduce false activations and to maintain the visual aesthetics of an on-screen keyboard, we chose the size of each target to be 84 pixels square. Furthermore, the keys are separated by a 12 pixel margin which further decreases the instances of false activations. We also show a bright red dot at the center of each of the on-screen buttons. These "focus points" (Figure 2) helps the users to focus their gaze at a point in the center of the target thereby improving the accuracy of the tracking data [22].

It should be noted that our on-screen layout does not conform exactly to a standard keyboard layout. A standard QWERTY layout has a maximum of 14 keys in a row. At a width of 84 pixels it would be possible to fit all 14 keys and maintain a QWERTY layout if we used all of the horizontal screen real-estate on the eye-tracker (1280x1024 resolution). We chose to implement a more compact layout which occupies less screen real-estate.

Previous research [24-26] has shown that the ideal duration for activation by dwell is on the order of 400-500ms. Consequently, we chose 450ms for our implementation, with an inter-dwell pause of 150ms. An audio beep provides users with feedback when a dwell-based activation is registered.

Our implementation shows both the standard characters and the shifted characters on-screen and provides no visual feedback for the activation of the shift key.

Gaze data from the eye tracker is noisy due to errors in tracking and also due to the physiology of the eye. We therefore implemented a saccade[1] detection and fixation smoothing algorithm [20] to provide more reliable data for detecting fixations.

7. Evaluation

To evaluate EyePassword, we conducted user studies with 18 subjects, 9 males and 9 females with an average age of 21. 13 subjects did not require any vision correction; 5 subjects used contact lenses[2]. Twelve subjects reported that they were touch-typists. On average subjects had 12 years of experience using a keyboard and mouse.

Our experimental setup used a standard office ergonomics setup with a desk and chair. The eye tracker is built into the screen and therefore imposed no additional encumbrances upon the users. Users could simply sit in front of the system, perform a one-time calibration and then begin using the system.

We compared the password entry speed and error rates of three approaches: a standard keyboard for entering a password (Keyboard) to provide a baseline, using EyePassword with dwell-based activation (Gaze+Dwell) and using EyePassword with

[1] A saccade is a ballistic movement of the eye used to reposition the visual focus to a new location in the visual environment.

[2] The eye tracker does work with eye-glasses provided the glasses do not occlude/impair the camera's view of the eye. We have had subjects with eye-glasses in previous studies.

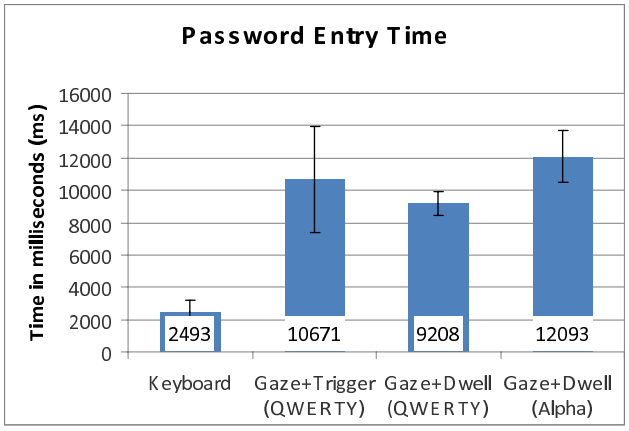

Figure 3. Average time for password entry across all users in each of the 4 conditions. Differences between Gaze+Dwell and Gaze+Trigger are not significant. Differences between QWERTY and alpha layouts are significant.

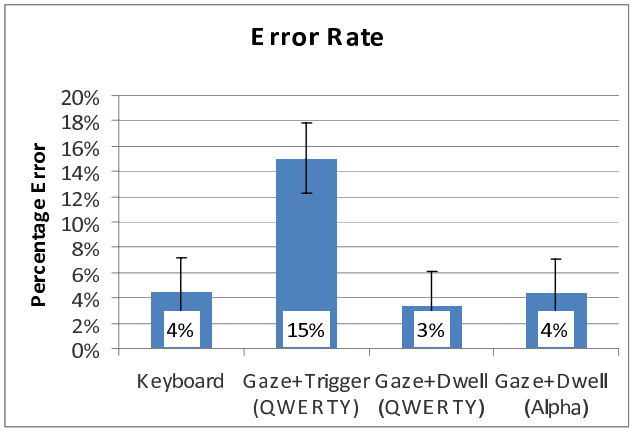

Figure 4. Percentage error in password entry across all users in each of the four conditions. Error rates in the Gaze+Dwell conditions were similar to those of the keyboard. Gaze+trigger error rates were considerably higher presumably due to eye-hand coordination.

trigger-based activation (Gaze+Trigger). In addition, we evaluated two different on-screen layouts for the dwell case: QWERTY layout and alphabetic layout.

At the end of the study we asked subjects to fill out a survey to collect data on the user's subjective opinion of the techniques.

7.1 Method

We implemented a test harness to capture timing and error data for users entering passwords in a controlled environment. To minimize any cognitive/memory effects, the users were shown the password in a dialog box immediately before they were asked to enter it. Each subject was first trained on the four test conditions: Keyboard, Gaze+Trigger (QWERTY layout), Gaze+Dwell (QWERTY layout) and Gaze+Dwell (Alphabetic layout). Subjects were trained on using each of the techniques on a practice set of four passwords which exercised the use of letters, numbers, upper-case and lower-case characters and symbols. Once subjects were comfortable with each approach, they repeated the trials with the real password data set of ten passwords shown below. Passwords were chosen to be representative of common passwords with a length of 8-9 characters and included a combination of lowercase, uppercase, numbers and symbols.

Training set: password, number1, capitalA, $symbol

Real set: computer, security, apple314, sillycat, Garfield, password, $dollar$, GoogleMap, dinnertime, Chinatown.

The order of the techniques was varied for each subject in order to counterbalance across subjects and to minimize learning effects. We measured the amount of time it took the user to enter each password. If the password was entered incorrectly, this was recorded as an error and the trial was repeated. Upon completion of the study, subjects were asked to provide their subjective opinions on the techniques used.

7.2 Results

Figure 3 shows the average time to enter the password in each of the four conditions. Figure 4 shows the percentage error in each condition.

A repeated measures analysis of variance (ANOVA) of the password entry time shows that the results are significant ($F(1.44,24.54)=117.8$, $p<.01$, Greenhouse-Geisser corrected). Contrast analyses between the four techniques showed that the differences between the keyboard and all the gaze based techniques are significant. While the average typing time for the trigger-based approach was higher than the dwell-based approach, this result was not significant - some users were faster using dwell, others using the trigger. The differences between the QWERTY layout and the alphabetic layout were significant indicating that users found the QWERTY layout faster.

The error rates on Gaze+Dwell (QWERTY) and Gaze+Dwell (Alpha) were similar to those on a keyboard. The trigger-based approach had a significantly higher error rate.

Our subjective evaluation showed that subjects unanimously preferred using the QWERTY layout over the alphabetic layout. Subjects did not indicate that the time to enter the password using the gaze-based approaches was a concern. The subjective results for the trigger mechanism (dwell-based or trigger-based) were counter to the results from our objective evaluation – a majority (>60%) of subjects felt that the trigger approach was faster and more accurate than using dwell. Subjects overwhelmingly (>80%) indicated that they would prefer to use a gaze-based approach over using a traditional keyboard when entering their password in a public place.

8. Discussion

While the speed difference between using dwell or trigger is inconclusive, our results do show that the error rates with the trigger approach are significantly higher (15% compared to 3-4%). Our hypothesis is that this is because it is difficult for humans to time their eye gaze and hand to coordinate perfectly. Most errors in the trigger condition occurred because either the

subjects had not yet focused on the target or had already moved their eyes off the target by the time they pressed the trigger. While we suspect that this behavior can probably be corrected for algorithmically, under the current implementation the dwell based implementation is more robust.

Our results also showed that the QWERTY layout outperformed the alphabetic keyboard layout. This indicates that the visual search time for finding characters on a QWERTY layout is lower than the visual search time for an alphabetic layout due to the fact that people have extensive training on the QWERTY layout.

Our study for entering passwords using a keyboard did not account for the increase in speed seen as a result of subjects developing muscle memory over time by entering their password repeatedly. We expect that similar to the muscle memory for typing passwords, learning effects for visual search on the on-screen layout will speed up password entry over time as subjects develop muscle memory in their eyes to enter their password.

When compared to password-entry time with the keyboard the gaze based approaches are about five times slower. However, it should be noted that even at an average of a 10 second entry time, the gaze-based password entry is several times faster than alternative techniques to prevent shoulder surfing [16, 17, 31, 36, 39, 40].

An additional security benefit of EyePassword is that the system never generates keyboard or mouse events during password entry. As a result, a present day keylogger cannot steal the users password. Of course, if our system is widely adopted, keyloggers can adapt to steal passwords from the eye tracker directly.

9. Future Work

We can strengthen a password by extracting a few additional entropy bits from the gaze path that the user follows while entering the password. Supposedly, the user will follow a similar path, with similar dwell times, every time. A different user, however, may use completely different dwell times. As a result, stealing the user's password is insufficient for logging in and the attacker must also mimic the user's gaze path. A similar technique was previously used successfully to enhance the entropy of passwords entered on a keyboard [27].

While our results showed that the trigger-based mechanism had considerably higher error rates due to eye-hand coordination, it is conceivable that this can be accounted for algorithmically by examining the historical gaze pattern and correlating it with trigger presses.

10. CONCLUSION

Passwords possess many useful properties as well as widespread legacy deployment, consequently we can expect their use for the foreseeable future. Unfortunately, today's standard methods for password input are subject to a variety of attacks based on observation, from casual eavesdropping (shoulder surfing), to more exotic methods. We have presented an alternative approach to password entry, based on gaze, which deters or prevents a wide range of these attacks. We have demonstrated through user studies that our approach requires marginal additional entry time, has accuracy similar to traditional keyboard input, while providing an experience preferred by a majority of users.

REFERENCES

1. *Apple MacBook iSight camera*. Apple Computer: Cupertino, California, USA. http://www.apple.com/macbook/isight.html
2. *The EyeGaze Communication System*, 2007. LC Technologies, Inc.: McLean, Virginia. http://www.eyegaze.com/2Products/Disability/Disabilitymain.htm
3. *IPRIZE: a $1,000,000 Grand Challenge designed to spark advances in eye-tracking technology through competition*, 2006. http://hcvl.hci.iastate.edu/IPRIZE/
4. *MyTobii Communication Software*, 2006. Tobii Technology AB. http://www.tobii.com/default.asp?sid=555
5. *PassFaces: patented technology that uses the brain's natural power to recognize familiar faces*. PassFaces Corporation. http://www.passfaces.com/products/passfaces.htm
6. *Schlage Scramble Keypad Reader (SERIII-W)*. Schlage (Ingersoll Rand Security Technologies). http://securitymanagementsystem.schlage.com/documents/readers_SERIII-W.pdf
7. Amir, A., M. Flickner, and D. Koons, Theory for Calibration Free Eye Gaze Tracking. 2002, IBM Almaden Research.
8. Amir, A., L. Zimet, A. Sangiovanni-Vincentelli, and S. Kao. An Embedded System for an Eye-Detection Sensor. *Computer Vision and Image Understanding, CVIU Special Issue on Eye Detection and Tracking* 98(1). pp. 104-23, 2005.
9. Asonov, D. and R. Agrawal. Keyboard Acoustic Emanations. In Proceedings of *IEEE Symposium on Security and Privacy*. Oakland, California, USA: IEEE. pp. 3-11, 2004.
10. Berger, Y., A. Wool, and A. Yeredor. Dictionary Attacks Using Keyboard Acoustic Emanations. In Proceedings of *Computer and Communications Security (CCS)*. Alexandria, Virginia, USA, 2006.
11. Duchowski, A. T., *Eye Tracking Methodology: Theory and Practice*: Springer. 227 pp. 2003.
12. Golle, P. and D. Wagner, *Cryptanalysis of a Cognitive Authentication Scheme*, International Association for Cryptologic Research, July 31 2006.
13. Hansen, D. W., D. MacKay, and J. P. Hansen. Eye Tracking off the Shelf. In Proceedings of *ETRA: Eye Tracking Research & Applications Symposium*. San Antonio, Texas, USA: ACM Press. pp. 58, 2004.
14. Hansen, J. P., K. Torning, A. S. Johansen, K. Itoh, and H. Aoki. Gaze Typing Compared with Input by Head and Hand. In Proceedings of *ETRA: Eye Tracking Research & Applications Symposium*. San Antonio, Texas, USA: ACM Press. pp. 131-38, 2004.
15. Henessey, C., B. Noureddin, and P. Lawrence. A Single Camera Eye-Gaze Tracking System with Free Head Motion. In Proceedings of *ETRA: Eye Tracking Research and Applications Symposium*. San Diego, California, USA: ACM Press. pp. 87-94, 2006.
16. Hoanca, B. and K. Mock. Screen Oriented Technique for Reducing the Incidence of Shoulder Surfing. In Proceedings of *International Conference on Security and Management (SAM)*. Las Vegas, Nevada, USA, 2005.
17. Hoanca, B. and K. Mock. Secure Graphical Password System for High Traffic Public Areas. In Proceedings of *ETRA - Eye Tracking Research and Applications Symposium*. San Diego, California, USA: ACM Press. pp. 35, 2006.

18. Jacob, R. J. K. and K. S. Karn, Eye Tracking in Human-Computer Interaction and Usability Research: Ready to Deliver the Promises, in *The Mind's eye: Cognitive and Applied Aspects of Eye Movement Research*, J. Hyona, R. Radach, and H. Deubel, Editors. Elsevier Science: Amsterdam. pp. 573-605, 2003.
19. Kuhn, M. G., Electromagnetic Eavesdropping Risks of Flat-Panel Displays, in *4th Workshop on Privacy Enhancing Technologies, LNCS*. Springer-Verlag: Berlin / Heidelberg. pp. 23–25, 2004.
20. Kumar, M., *GUIDe Saccade Detection and Smoothing Algorithm*. Technical Report CSTR 2007-03, Stanford University, Stanford 2007. http://hci.stanford.edu/cstr/reports/2007-03.pdf
21. Kumar, M., *Reducing the Cost of Eye Tracking Systems*. Technical Report CSTR 2006-08, Stanford University, Stanford, April 2006. http://hci.stanford.edu/cstr/reports/2006-08.pdf
22. Kumar, M., A. Paepcke, and T. Winograd. EyePoint: Practical Pointing and Selection Using Gaze and Keyboard. In Proceedings of *CHI*. San Jose, California, USA: ACM Press, 2007.
23. Maeder, A., C. Fookes, and S. Sridharan. Gaze Based User Authentication for Personal Computer Applications. In Proceedings of *International Symposium on Intelligent Multimedia, Video and Speech Processing*. Hong Kong: IEEE. pp. 727-30, 2004.
24. Majaranta, P., A. Aula, and K.-J. Räihä. Effects of Feedback on Eye Typing with a Short Dwell Time. In Proceedings of *ETRA: Eye Tracking Research & Applications Symposium*. San Antonio, Texas, USA: ACM Press. pp. 139-46, 2004.
25. Majaranta, P., I. S. MacKenzie, A. Aula, and K.-J. Räihä. Auditory and Visual Feedback During Eye Typing. In Proceedings of *CHI*. Ft. Lauderdale, Florida, USA: ACM Press. pp. 766-67, 2003.
26. Majaranta, P. and K.-J. Räihä. Twenty Years of Eye Typing: Systems and Design Issues. In Proceedings of *ETRA: Eye Tracking Research & Applications Symposium*. New Orleans, Louisiana, USA: ACM Press. pp. 15-22, 2002.
27. Monrose, F., M. K. Reiter, and S. Wetzel. Password hardening based on keystroke dynamics. *International Journal of Information Security* 1(2). pp. 69-83, 2002.
28. Morimoto, C., D. Koons, A. Amir, and M. Flickner. Pupil Detection and Tracking Using Multiple Light Sources. *Image and Vision Computing* 18(4). pp. 331-36, 2000.
29. Morimoto, C. H., A. Amir, and M. Flickner. Free Head Motion Eye Gaze Tracking Without Calibration. In Proceedings of *CHI*. Minneapolis, Minnesota, USA: ACM Press. pp. 586-87, 2002.
30. Ohno, T. and N. Mukawa. A Free-head, Simple Calibration, Gaze Tracking System That Enables Gaze-Based Interaction. In Proceedings of *ETRA: Eye Tracking Research & Applications Symposium*. San Antonio, Texas, USA. pp. 115-22, 2004.
31. Roth, V., K. Richter, and R. Freidinger. A PIN-Entry Method Resilient Against Shoulder Surfing. In Proceedings of *CCS: Conference on Computer and Communications Security*. Washington DC, USA: ACM Press. pp. 236-45, 2004.
32. RSA Security, I., *RSA SecurID Authentication*. http://www.rsasecurity.com/node.asp?id=1156
33. Simonite, T. Tactile passwords could stop ATM 'shoulder-surfing', *New Scientist*, October 6, 2006.
34. Song, D. X., D. Wagner, and X. Tian. Timing Analysis of Keystrokes and Timing Attacks on SSH. In Proceedings of *10th USENIX Security Symposium*. Washington DC, USA: The USENIX Association, 2001.
35. Suo, X. and Y. Zhu. Graphical Passwords: A Survey. In Proceedings of *Annual Computer Security Applications Conference*. Tucson, Arizona, USA, 2005.
36. Tan, D. S., P. Keyani, and M. Czerwinski. Spy-Resistant Keyboard: Towards More Secure Password Entry on Publicly Observable Touch Screens. In Proceedings of *OZCHI - Computer-Human Interaction Special Interest Group (CHISIG) of Australia*. Canberra, Australia: ACM Press, 2005.
37. Thorpe, J., P. C. van Oorschot, and A. Somayaji. Pass-thoughts: authenticating with our minds. In Proceedings of *New Security Paradigns Workshop*. Lake Arrowhead, California, USA: ACM Press. pp. 45-56, 2005.
38. Tobii Technology, AB, *Tobii 1750 Eye Tracker*, 2006. Sweden. http://www.tobii.com
39. Weinshall, D. Cognitive Authentication Schemes Safe Against Spyware (Short Paper). In Proceedings of *IEEE Symposium on Security and Privacy*. Oakland, California, USA: IEEE, 2006.
40. Wiedenbeck, S., J. Waters, L. Sobrado, and J.-C. Birget. Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme. In Proceedings of *AVI*. Venezia, Italy: ACM Press. pp. 177-84, 2006.
41. Zhu, Z., K. Fujimura, and Q. Ji. Real-Time Eye Detection and Tracking Under Various Light Conditions. In Proceedings of *ETRA: Eye Tracking Research & Applications Symposium*. New Orleans, Louisiana, USA: ACM Press. pp. 139-44, 2002.
42. Zhuang, L., F. Zhou, and J. D. Tygar. Keyboard Acoustic Emanations Revisited. In Proceedings of *Computer and Communications Security (CCS)*. Alexandria, Virgina, USA: ACM Press. pp. 373-82, 2005.