ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

Shoulder Surfing Resistant and Graphical Authentication System

R.Ananda Padmanathan[1], K.Rajmohan[2], S.Jeyajeevanram[3] , S.John Joseph[4], S.Saravanakumar[5]

Department of Computer Science and Engineering, Sudharsan Engineering College, Sathiyamangalam, Pudukkottai, TamilNadu, India [1,2,3]

Assistant Professor, Department of Computer Science and Engineering, Sudharsan Engineering College, Sathiyamangalam, Pudukkottai, TamilNadu, India[4,5]

ABSTRACT: Shoulder surfing or adversarial eavesdropping to infer users' keystrokes on physical QWERTY keyboards continues to be a serious privacy threat. Despite this, practical and efficient countermeasures against such attacks are still lacking. In this paper, we propose keyboard randomization as a simple, yet effective, countermeasure against various types of keystroke inference attacks. Our proposal consists of several keyboard randomization strategies which randomizes or changes the position of keys on the keyboard. The randomized keyboard is then projected to the typing user by means of an augmented reality wearable device. As the randomized keyboard is visually superimposed over the actual physical keyboard, and is visible only to the typing user through the augmented reality device, it acts as an effective countermeasure against both side-channel and visual-channel based keystroke inference attacks. We implement our proposed solution on a commercially available augmented reality device and conduct preliminary evaluations to validate its performance and effectiveness. Index Terms—Eavesdropping, keystroke inference, random keyboard, augmented reality

I. INTRODUCTION

Physical **QWERTY** keyboards are the most widely adopted input interface for personal and portable computing systems. These keyboards have also been a constant target for various forms of "shoulder surfing" attacks, where the goal of an adversary is to obtain or infer users' keystrokes by directly, surreptitiously, observing the typing user (and the keyboard) but or eavesdropping on certain information directly related to the typing activity being performed. The first case, where the adversary has a covert visual access to the typing user, is a more common and easy-to-execute threat. Such threats are also the most difficult to protect against, especially by means of traditional cryptography-based or other information manipulation and hiding techniques. For instance, Roth et al. [1] proposed an oracle-based multi-round protocol for PIN entry by color coding keys into two shades (black and white). This scheme takes advantage of limitations in human cognitive capabilities to overcome shoulder surfing, however, Kwon et al. [2] recently showed that covert attention and perceptual grouping can improve information processing by humans, thus rendering Roth et al.'s approach ineffective. Alternatively, there exists other forms of shoulder surfing attacks that, rather than relying on the direct visual channel, take advantage of indirect information channels (or side-channels) to infer users' keystrokes. For instance, Vuagnoux et al. [3]

use electromagnetic emanations from external keyboards (both wired and wireless) to infer keystrokes, whereas, Berger et al. [4] have accomplished a similar feat by using acoustic emanations originating due to typing on these keyboards. variation of non-visual shoulder surfing, Marquardt et al. [5] utilized the vibrations sensed by a smartphone accelerometer (positioned in the proximity of the target keyboard) to infer a users' keystrokes on the keyboard. Maiti et al. [6] proposed a similar attack by taking advantage of motion information available from wrist-wearable devices such as smartwatches. More recently, Ali et al. [7] demonstrated the ability to infer keystrokes by observing the unique changes in the radio signal channel statistics caused during typing. Interestingly, the success of all of the above attacks rely

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

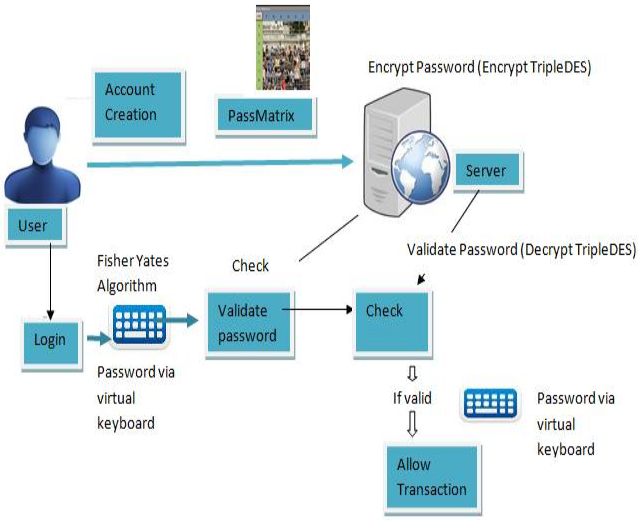

Fig.1 Proposed System Architecture

II. EASE OF USE

In this paper, we overcome the above technical challenges and propose a system for randomizing external keyboard layouts by making a novel and interesting use of augmented reality devices. One key advantage of our proposal is that it is able to overcome all forms of shoulder surfing attacks, including those possible through direct visual access of the target keyboard. Our proposal consists of several keyboard layout randomization strategies, each of which assigns a unique non-standard position to the keys on the keyboard which is unknown to the adversary. The randomized keyboard is then projected to the typing user by means of an augmented reality wearable device. As the randomized keyboard is visually superimposed over the actual physical keyboard, and is visible only to the typing user through the augmented reality device, it acts as an effective countermeasure against both side-channel and visual channel-based keystroke inference or shoulder surfing attacks. We implement our system on the commercially available EPSON Moverio BT-200 [10] augmented reality device and validate its performance and effectiveness by means of preliminary empirical usage data from a small number of test subjects.

A. Randomization Strategies To prevent keystroke inference attacks, an important task in the proposed system is to ensure that the layout of the augmented characters is unpredictably different from the default QWERTY layout. Moreover, as an adversary can gain semantic knowledge from multiple observations and re-train his attack framework, changing the augmented keyboard layout just once (or in a very predictable or insignificant fashion) will not be an effective defense. To prevent an adversary from knowing the keyboard layout in use at any given time, the change in layout should be randomized. Accordingly, in our proposed system, every time the user wants to type sensitive text, a newly randomized keyboard layout is augmented over the physical keyboard. The new mapping of the randomized layout to the underlying physical keys is also updated accordingly on the computer side by means of the secure communication link. In this paper, we focus on randomization of just the twenty-six alphabets (Figure 2), however it could be easily extended to all keys. Below, we list a few representative (by no means an exhaustive list) randomization strategies that can be used to change the keyboard layout:

(i) **Individual Key Randomization (IKR):** This strategy randomly assigns positions to each alphabet or letter on the augmented keyboard layout, without any relation to its actual position on the QWERTY layout.

(ii) Row Shifting (RS): In this strategy, the alphabets in each row of the QWERTY layout (rows in Figure 2) are circularly left or right shifted by a random number of keys

(iii) Column Shifting (CS): In this strategy, the alphabets in each column of the **QWERTY** layout (columns in Figure 2) are circularly top or bottom shifted by a random number of keys on the augmented layout. In other words,

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

in CS each alphabet on the augmented layout is found on the same column as in the **QWERTY** layout, however its position is shifted top or bottom by a random number. As the column (correspondingly, row in RS) of each alphabet and the order of alphabets in each column (correspondingly, row in RS) is maintained comparatively alphabet on the CS and RS layouts. **B. Security Analysis** : As the keyboard layout is randomized, the best an adversary (assumed to know the randomization strategy used by it's target) can do is guess the mapping between the randomized and **QWERTY** layouts. We use the successful guessing probability to indicate the level of security assurance each randomization strategy provides in the presence of an eavesdropping adversary. For a particular randomization strategy, the lower this probability is, the higher the security assurance provided by it. In IKR, the probability that an adversary correctly guesses the mapping of a particular alphabet is 1 26 , i.e., uniformly distributed. Moreover, the probability that the adversary guesses the entire mapping correctly is 1 26! = 2.4 × 10−27, which is negligibly small. However, in case of RS and CS, the adversary can improve it's guessing, based on the relative positioning of key within a row and column, respectively. Knowing that keys within a shifted row remain in (circular) order, for a row shifted keyboard (RS), the adversary only needs to guess the random length of shifting. The probability that an adversary correctly guesses the length of a row's shifting is 1 10 , 1 9 , and 1 7 , for rows 1, 2, 3, respectively (as labeled in Figure 2). Therefore, the probability that the adversary guesses the mapping for all 26 alphabets correctly is 1 10 × 1 9 × 1 7 = 1.5 × 10−3 .

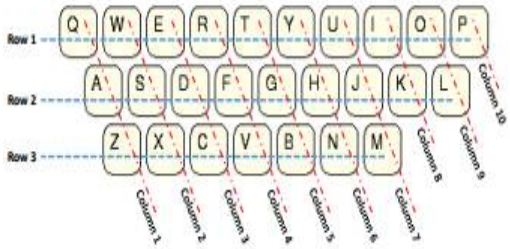

Fig. 2. Assumed rows and columns for RS and CS strategies.

(a) **Literature Survey**

The participants were directed with audio-visual instructions on what to type on the keyboard. In the first part of the experiment, each participant typed all twenty six alphabets of English language in random order. In the second part of the experiment, each participant typed five familiar words: first name, last name, hometown, address street, and area of work. In the third part of the experiment, each participant typed an experimental password of their choice. For the second and third parts, ground truth was collected beforehand, in order to calculate typing accuracy

Accuracy: The average typing accuracy for all thirteen participants in typing a key on the default **QWERTY** keyboard (with augmentation turned off) was 94.37%, 93.78%, and 99% for random letters, familiar words, and password, respectively. When the randomized keyboard augmentation was turned on with the IKR randomization strategy, the average accuracy for all thirteen participants in typing a key dropped marginally to 93.19%, 93.19%, 98.53%, respectively. However, typing accuracies in CS (92.89%, 94.08%, 98.53%) and RS (93.78%, 94.37%, 97.76%) randomization strategies were similar to the **QWERTY** keyboard, if not better. Averaged results from each typing scenario are presented in Figure 6b. After the experiment was completed, one of the participants expressed concerns about the lag in rendering of the keys, especially noticeable when the user moves his/her head. The delay in rendering may have confused the participants, and lead to longer task completion times and/or more errors in typing. Therefore, results suggest that if some of the issues with our proof-of-concept prototype are resolved, typing accuracy can be comparable to typing on default QWERTY keyboards. Readers may notice that password typing took the longest and was also more accurately typed than the random letters and familiar words. This occurrence is primarily because the participants had to carefully recall and type the experimental password (chosen at the beginning of the study), which most likely is not one of the passwords they use in real-life. Perceived Task Load: The NASA-TLX is a

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

multidimensional scale to measure the perceived workload, including, the mental, physical and temporal demand, overall performance, frustration level and effort. We employ this scale in our experiments to capture the task load imposed on participants in using the augmented random keyboard. Figure 6c shows the average overall score as well as the six individual subscales. Using augmented random keyboard was perceived by participants to be mentally demanding and complex (59.61 - Mental). Participants also felt that the task required significant effort to accomplish (61.61 - Effort). Participants were also not entirely satisfied with the performance of our implementation (27.76 - Perform). However, the physical activity required and time pressure felt due to the pace at which the tasks were being completed are notably low (30.07 - Physical, 37.53 - Temporal). Participants felt moderately content, relaxed, and complacent during the task (44.07 - Frustration).screen in the background. We chose to use the Anker A7726121 Bluetooth keyboard because of its generic design. The keyboard was connected to the computer and the alphabet keys were covered with corresponding alphabetic markers (Figure 3). As a result, the keyboard was usable even as a regular **QWERTY** keyboard. Participants wore the EPSON BT-200 augmented reality device during the experiment. The EPSON BT-200 is equipped with a front facing camera with a resolution of 640×480 pixels, which enables augmented reality applications. The BT-200 also features the Android 4.1 platform, and our implementation of the augmented randomized keyboard was installed as an application. Our implementation of the augmented randomized keyboard uses the ARToolKit library

The following figure illustrates the authentication window of the proposed system.

Fig. 5. A participant typing on the randomized augmented keyboard.

Fig. 3. A QWERTY keyboard with alphabetic markers glued on top of the corresponding alphabet keys.

Fig. 4. An instance of an augmented keyboard with IKR strategy as observed by the typer on the EPSON Moverio BT-200.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

III. CONCLUSION

Generalization to Other Keyboards: One advantage of our proposed design is that it can be easily generalized and deployed across different types of keyboards/keypads. The use of character recognition, instead of the exemplary marker recognition used in our prototype, will enable such a generalized design. One application of such a generalized design can be found in ATM machines. Numeric keypads on ATMs, due to their open or unrestricted locations, are the most prone to shoulder surfing attacks. The proposed system could be used in this scenario, where a users' augmented reality device could communicate with the ATM by meansof a secured wireless channel to exchange a per-transaction randomized layout. This layout can then be augmented over the actual numeric keypad of the ATM machine and made visible only to the user by means of his/her augmented reality device

REFERENCES

[1] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry Method Resilient Against Shoulder Surfing," in ACM CCS 2004.
[2] T. Kwon, S. Shin, and S. Na, "Covert Attentional Shoulder Surfing: Human Adversaries Are More Powerful than Expected," IEEE Transactions on SMC: Systems, vol. 44, no. 6, 2014.
[3] M. Vuagnoux and S. Pasini, "Compromising electromagnetic emanations of wired and wireless keyboards," in USENIX Security 2009.
[4] Y. Berger, A. Wool, and A. Yeredor, "Dictionary Attacks using Keyboard Acoustic Emanations," in ACM CCS 2006.
[5] P. Marquardt, A. Verma, H. Carter, and P. Traynor, "(sp)iPhone: Decoding Vibrations from Nearby Keyboards using Mobile Phone Accelerometers," in ACM CCS 2011.
[6] A. Maiti, O. Armbruster, M. Jadliwala, and J. He, "Smartwatch-Based Keystroke Inference Attacks and Context-Aware Protection Mechanisms," in ACM ASIACCS 2016.
[7] K. Ali, A. X. Liu, W. Wang, and M. Shahzad, "Keystroke Recognition using WiFi Signals," in ACM MobiCom 2015.
[8] Software House, "Scramble Keypad SP-100," www.swhouse.com/products.
[9] Y. S. Ryu, D. H. Koh, B. L. Aday, X. A. Gutierrez, and J. D. Platt, "Usability Evaluation of Randomized Keypad," Journal of Usability Studies, vol. 5, no. 2, pp. 65–75, 2010.
[10] EPSON, "Moverio BT-200," www.epson.com/MoverioBT200.
[11] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing Shoulder-Surfing by Using Gaze-Based Password Entry," in ACM SOUPS 2007.
12] Passfaces, "Two Factor Authentication - Graphical Passwords," www.realuser.com.
[13] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in USENIX Security 1999.
[14] F. Tari, A. Ozok, and S. H. Holden, "A Comparison of Perceived and Real Shoulder-Surfing Risks Between Alphanumeric and Graphical Passwords," in ACM SOUPS 2006.
{15] Y. Zhang, P. Xia, J. Luo, Z. Ling, B. Liu, and X. Fu, "Fingerprint Attack Against Touch-enabled Devices," in ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, 2012.
[16] A. H. Lashkari, A. Abdul Manaf, M. Masrom, and S. M. Daud, DICTAP 2011. Springer, ch. Security Evaluation for Graphical Password.
[17] Q. Yan, J. Han, Y. Li, J. Zhou, and R. H. Deng, "Designing Leakageresilient Password Entry on Touchscreen Mobile Devices," in ACM ASIACCS 2013. [18] D. F. Abawi, J. Bienwald, and R. Dorner, "Accuracy in Optical Tracking with Fiducial Markers: An Accuracy Function for ARToolKit," in ACM ISMAR 2004.
[19] H. Kato, "Inside ARToolKit," in 1st IEEE International Workshop on Augmented Reality Toolkit, 2007.
[20] R. A. Bailey, Design of comparative experiments. Cambridge University Press, 2008, vol. 25.
[21] S. G. Hart and L. E. Staveland, "Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research," Advances in Psychology, vol. 52, pp. 139–183, 1988.
[22] J. Brooke, "SUS - A Quick and Dirty Usability Scale," Usability Evaluation in Industry, 1996.

[