International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 9 Issue 5 ǁ 2021 ǁ PP. 45-48

Efficient Password Mechanism to Overcome Spyware Attacks

AUTHOR:Varsha M, Nivethitha R,(GuideMrs. Sangeetha Krishnan)

ABSTRACT:
This work enhances traditional authentication systems based on Personal Identification Numbers (PIN) and One- Time Passwords (OTP) through the incorporation of biometric information as a second le0vel of user authentication. In our proposed approach, users draw each digit of the password on the touchscreen of the device instead of typing them as usual. A complete analysis of our proposed biometric system is carried out regarding the discriminative power of each handwritten digit and the robustness when increasing the length of the password and the number of enrolment samples. The new e-BioDigit database, which comprises on-line handwritten digits from 0 to 9, has been acquired using the finger as input on a mobile device. This database is used in the experiments reported in this work and it is available together with benchmark results in GitHub1. Finally, we discuss specific details for the deployment of our proposed approach on current PIN and OTP systems, achieving results with Equal Error Rates (EERs) ca. 4.0% when the attacker knows the password. These results encourage the deployment of our proposed approach in comparison to traditional PIN and OTP systems where the attack would have 100% success rate under the same impostor scenario

---

Date of Submission: 27-04-2021 Date of acceptance: 11-05-2021

I. INTRODUCTION

The rapid and continuous deployment of mobile devices around the world has been motivated not only by the high technological evolution that allows the communication and use of social media in real time, the two most prevalent user authentication approaches have been Personal Identification Numbers and One-Time Passwords. In our proposed approach, users draw each digit of the password on the touch screen of the device instead of typing them as usual. The handwritten digits can be first recognized using for example an Optical Character Recognition. After this first authentication stage, the biometric information of the handwritten digits is compared in a second authentication stage to the enrolment data of the claimed user, comparing each digit one by one.

II. LITERATURE SURVEY

[1] Title: Online Signature Verification on Mobile Devices.Authors: N.Sae-Bae and N.Memon. Published Year: 2014.Description: This paper investigates multitouch gestures for user authentication on touch sensitive devices. A canonical set of 22 multitouch gestures was defined using characteristics of hand and finger movement. Then, a multitouch gesture matching algorithm robust to orientation and translation was developed. Two different studies were performed to evaluate the concept.
Efficiency: It is noticed that performing a user-defined gesture over a customized background image does result in higher verification performance.
[2]Title:User Verification Using Safe Handwritten Passwords on Smartphones. Authors: T. Kutzner,
F.Ye,
I.Bonninger,
C. Travieso,
M. Dutta,
and A. Singh .Published Year: 2015 Description: In this work, in an attempt to become the first research-embedded approach to smartphone vein identification, a novel wrist vascular biometric recognition is designed, implemented, and tested on the Xiaomi© Pocophone F1 and the Xiaomi© Mi 8 devices.
Efficiency: In this paper, a novel contactless vascular biometric recog-
nition system for wrist vein modality has been created, tested, and completely embedded into a smartphone. The non-contact interaction with the smartphone, intended for screen unlocking and more secure online payments, has been the motivation behind this work.
[3]Title:Graphical Password based User Authentication with Free-Form Doodles.Authors: M.Martinez-Diaz, J. Fierrez, and J. Galbally. Published Year: 2016 Description: In this work, authentication with free-form sketches is studied. Verification systems using dynamic time warping and Gaussian mixture models are proposed, based on dynamic signature verification approaches. The most discriminant features are studied using the sequential forward floating selection algorithm.

Efficiency:The best performing systems against random and skilled forgeries were tuned for each scenario respectively, and fusion of both systems provided an overall good performance in both scenarios. In our case, score fusion also provides better results than individual systems.

[4] Title: BioTouchPass: Handwritten Passwords for Touchscreen Biometrics.Authors: Ruben Tolosana, Ruben Vera-Rodriguez, Member, IEEE, and Julian Fierrez, Member, IEEE.Published Year:2020 Description: This work enhances traditional authentication systems based on Personal Identification Numbers (PIN) and One Time Passwords (OTP) through the incorporation of biometric information as a second level of user authentication. In our proposed approach, users draw each digit of the password on the touchscreen of the device instead of typing them as usual.Efficiency: proposed approach achieves good results with EERs ca. 4.0% when considering imitation attacks, outperforming other traditional biometric verification traits such as the handwritten signature or graphical passwords on similar mobile scenarios. Additionally, we discuss specific details for the deployment or our proposed approach on current PIN- and OTP-based authentication systems.

III. PROPOSED SYSTEM

Our proposed system focuses on providing user-friendly mobile applications ensuring data protection and high security. Users should draw each digit of the password on the touch screen instead of typing them as usual. This way, the traditional authentication systems are enhanced by incorporating dynamic handwritten biometric information. Our system involves two stages of authentication: the drawn pin should be similar to the pin entered during the registration process.

Our second stage of authentication involves multiple options based on user preference where users can set multiple sets of combinations. Users can set a second stage password as stroke, time, screen brightness or sensor based authentication system. The incorporation of biometric information on traditional password-based systems can improve the security through a second level of user authentication.

IV. SYSTEM ARCHITECTURE

Users should draw each digit of the password on the touch screen instead of typing them as usual. This way, the traditional authentication systems are enhanced by incorporating dynamic handwritten biometric information. Our system involves two stages of authentication. The drawn pin should be similar to the pin entered during the registration process.

Our second stage of authentication involves multiple options based on user preference where users can set multiple sets of combinations. Users can set a second stage password as stroke, time, screen brightness or sensor based authentication system. The incorporation of biometric information on traditional password-based systems can improve the security through a second level of user authentication.

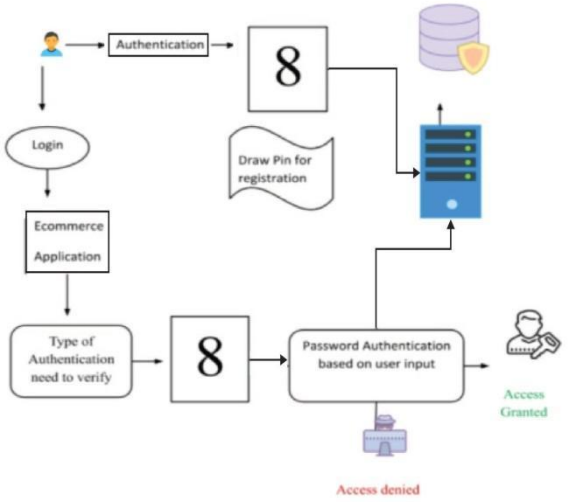

Fig 1. Block Diagram

V. MODULE DESCRIPTION

User Registration

User has an initial level Registration Process. The users provide their own personal information for this process. The server in turn stores the information in its database and the user can view a list of products in their page with multiple lists of products and their details.

Password Creation Using Strokes

Users can select a list of products they wish to purchase. The selected product will be listed in a cart page and the user can initiate general purchase information to be filled. Completing general detail, the user has to draw their four digit pin one by one on screen. The drawn password is then converted into an image through optical character recognition numbers from each image fetched and verified with the user password.

Product Selection And Payment Using Handwritten Password

User has to register their four digit password with multiple strokes during their registration process once the process is completed during confirm password...User has to confirm their password with the same password with stroke has to be verified. Strokes for each drawn digits should match with strokes given at time of registration.

Password Analysing

Spyware attack will be avoided by proposing the idea that uses the screen brightness as an authentication tool. The android secure environment generates the 6 digit binary value. Based on the binary digit the brightness of the screen gets changed to high or low. If the screen brightness is high the user should input the correct PIN digit. Else the user should give the wrong and random PIN number. The system will remove the digits which are inserted while the screen brightness is low and apply the HMac algorithm for the PIN given by the user and generate the Signature for the user PIN which is a digestible Value in order to avoid MAN-IN-MIDDLE attack. The server gets the signature of the user generated PIN and generates the signature value for the Original PIN and compares two signatures. If the two Signatures are equal the user can access the Profile of the user. If not, the user can't access the profile.

VI. SYSTEM IMPLEMENTATION

HARDWARE ENVIRONMENT

- Hard Disk:500GB and Above
- RAM:4 GB and Above
- Processor:I3 and Above

SOFTWARE ENVIRONMENT

- Windows 7 and above
- JDK 1.7
- Xampp
- Android Studio 3.4
- Android Phone

Technology Used:

- Core java, Android, PHP

VII. SCREENSHOT

Fig 2 .Optical Character Recognition

VIII. CONCLUSION

We propose the smart way to authenticate the social networking accounts belonging to them by using the screen brightness of android mobiles in order to avoid the spyware attack, shoulder surfing attack, and man in the middle attack.

REFERENCES

[1]. M. Salehan and A. Negahban, "Social Networking on Smartphones: When Mobile Phones Become Addictive," Computers in Human Behavior, vol. 29, no. 6, pp. 2632–2639, 2013.

[2]. J. Bonneau, C. Herley, P. Oorschot, and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," in Proc. IEEE Symposium on Security and Privacy, 2012, pp. 553–567.

[3]. J. Galbally, I. Coisel, and I. Sanchez, "A New Multimodal Approach for Password Strength Estimation Part I: Theory and Algorithms," IEEE Transactions on Information Forensics and Security, vol. 12, pp. 2829– 2844, 2017.

[4]. A. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. Smith, "Smudge Attacks on Smartphone Touch Screens," in Proc. of the 4th USENIX Conference on Offensive Technologies, 2010, pp. 1–7.

[5]. D. Shukla, R. Kumar, A. Serwadda, and V. Phoha, "Beware, Your Hands Reveal Your Secrets!" in Proc. of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014.

[6]. Q. Yue, Z. Ling, X. Fu, B. Liu, W. Yu, and W. Zhao, "My Google Glass Sees Your Passwords!" in Black Hat USA, 2014.

[7]. W. Meng, D. Wong, S. Furnell, and J. Zhou, "Surveying the Development of Biometric User Authentication on Mobile Phones," IEEE Communications Surveys Tutorials, vol. 17, no. 3, pp. 1268–1293, 2015.

[8]. L. Wan, M. Zeiler, S. Zhang, Y. LeCun, and R. Fergus, "Regularization of Neural Networks using DropConnect," in Proc. of the 30th International Conference on Machine Learning, 2013, pp. 1058–1066.

[9]. M. Liang and X. Hu, "Recurrent Convolutional Neural Network for Object Recognition," in Proc. of the IEEE Conference on Computer Vision and Pattern Recognition, 2015, pp. 3367–3375.

[10]. J. Angulo and E. Wastlund, "Exploring Touch-Screen Biometrics for User Identification on Smartphones," J. Camenisch, B. Crispo, S. Fischer-Hbner, R. Leenes, G. Russello (Eds.), Privacy and Identity Management for Life, Springer, pp. 130–143, 2011.

[11]. P. Lacharme and C. Rosenberger, "Synchronous One Time Biometrics With Pattern Based Authentication," in Proc. 11th Int. Conf. on Availability, Reliability and Security, ARES, 2016.

[12]. E. von Zezschwitz, M. Eiband, D. Buschek, S. Oberhuber, A. D. Luca, F. Alt, and H. Hussmann, "On Quantifying the Effective Password Space of Grid-based Unlock Gestures," in Proc. of the International Conference on Mobile and Ubiquitous Multimedia, 2016, pp. 201–212.

[13]. D. Buschek, A. D. Luca, and F. Alt, "There is more to Typing than Speed: Expressive Mobile Touch Keyboards via Dynamic Font Personalisation," in Proc. of the International Conference on Human- Computer Interaction with Mobile Devices and Services, 2015, pp. 125– 130.

[14]. ——, "Improving Accuracy, Applicability and Usability of Keystroke Biometrics on Mobile Touchscreen Devices," in Proc. of the CHI Conference on Human Factors in Computing Systems, 2015, pp. 1393–

[15]. L. Li, X. Zhao, and G. Xue, "Unobservable Reauthentication for Smartphones," in Proc. 20th Network and Distributed System Security Symposium, NDSS, 2013.

[16]. N. Sae-Bae, N. Memon, K. Isbister, and K. Ahmed, "Multitouch Gesture-Based Authentication," IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 568–582, 2014.

[17]. C. Shen, Y. Zhang, X. Guan, and R. Maxion, "Performance Analysis of Touch-Interaction Behavior for Active Smartphone Authentication," IEEE Transactions on Information Forensics and Security, vol. 11, no. 3, pp. 498–513, 2016.

[18]. J. Fierrez, A. Pozo, M. Martinez-Diaz, J. Galbally, and A. Morales, "Benchmarking Touchscreen Biometrics for Mobile Authentication," IEEE Trans. on Information Forensics and Security, vol. 13, 2018.

[19]. N. Sae-Bae and N. Memon, "Online Signature Verification on Mobile Devices," IEEE Transactions on Information Forensics and Security, vol. 9, no. 6, pp. 933–947, 2014.

[20]. R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega- Garcia, "Benchmarking Desktop and Mobile Handwriting across COTS Devices: the e-BioSign Biometric Database," PLOS ONE, 2017.

[21]. W. Khan, M. Aalsalem, and Y. Xiang, "A Graphical Password Based System for Small Mobile Devices," International Journal of Computer Science, vol. 5, no. 2, pp. 145–154, 2011.

[22]. M. Martinez-Diaz, J. Fierrez, and J. Galbally, "Graphical Password Based User Authentication with Free-Form Doodles," IEEE Trans. On Human-Machine Systems, vol. 46, no. 4, pp. 607–614, 2016.

[23]. T. Kutzner, F. Ye, I. Bonninger, C. Travieso, M. Dutta, and A. Singh, "User Verification Using Safe Handwritten Passwords on Smartphones," in Proc. 8th International Conference on Contemporary Computing, IC3, 2015.

[24]. T. Nguyen, N. Sae-Bae, and N. Memon, "DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices," Computers and Security, vol. 66, pp. 115–128, 2017.

[25]. R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "Incorporating Touch Biometrics to Mobile One-Time Passwords: Exploration of Digits," in Proc. IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2018.