IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 6, June 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006234|

Bio-Touch Pass: Efficient Password Mechanism to Overcome Spyware Attacks

Bharath.M[1] , Praveen.M[2] , Tharun Raj.Y[3], Shiny R.M[4]

UG Student, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India [1,2,3]

Assistant Professor, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India [4]

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 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. 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.

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

Project Title: Recurrent Convolutional Neural Network for Object Recognition
Author Name: Ming Liang Xiaolin Hu
Abstract
In recent years, the convolutional neural network (CNN) has achieved great success in many computer vision tasks. Partially inspired by neuroscience, CNN shares many properties with the visual system of the brain. A prominent difference is that CNN is typically feed-forward architecture while in the visual system recurrent connections are abundant. Inspired by this fact, we propose a recurrent CNN (RCNN) for object recognition by incorporating recurrent connections into each convolutional layer. Though the input is static, the activities of RCNN units evolve over time so that the activity of each unit is modulated by the activities of its neighboring units. This property enhances the ability of the model to integrate the context information, which is important for object recognition. Like other recurrent neural networks, unfolding the RCNN through time can result in an arbitrarily deep network with a fixed number of parameters. Furthermore, the unfolded network has multiple paths, which can facilitate the learning process. The model is tested on four benchmark object recognition datasets: CIFAR-10, CIFAR-100, MNIST and SVHN. With fewer trainable parameters, RCNN outperforms the state-of-the-art models on all of these datasets. Increasing the number of parameters leads to even better performance. These results demonstrate the advantage of the recurrent structure over purely feed-forward structure for object recognition.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006234|

Project Title: The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes

Author Name: Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajano

Abstract

We evaluate two decades of proposals to replace text passwords for general-purpose user authentication on the web using a broad set of twenty-five usability, deploy ability and security benefits that an ideal scheme might provide. The scope of proposals we survey is also extensive, including password management software, federated login protocols, graphical password schemes, cognitive authentication schemes, one-time passwords, hardware tokens, phone-aided schemes and biometrics. Our comprehensive approach leads to key insights about the difficulty of replacing passwords. Not only does no known scheme come close to providing all desired benefits: none even retains the full set of benefits that legacy passwords already provide. In particular, there is a wide range from schemes offering minor security benefits beyond legacy passwords, to those offering significant security benefits in return for being more costly to deploy or more difficult to use. We conclude that many academic proposals have failed to gain traction because researchers rarely consider a sufficiently wide range of real-world constraints. Beyond our analysis of current schemes, our framework provides an evaluation methodology and benchmark for future web authentication proposals.

Project Title: Benchmarking Touch screen Biometrics for Mobile Authentication

Author Name: Julian Fierrez

Abstract

We study user interaction with touch screens based on swipe gestures for personal authentication. This approach has been analyzed only recently in the last few years in a series of disconnected and limited works. We summarize those recent efforts, and then compare them to three new systems (based on SVM and GMM using selected features from the literature) exploiting independent processing of the swipes according to their orientation. For the analysis, four public databases consisting of touch data obtained from gestures sliding one finger on the screen are used. We first analyze the contents of the databases, observing various behavioral patterns, e.g., horizontal swipes are faster than vertical independently of the device orientation. We then explore both an intra-session scenario where users are enrolled and authenticated within the same day; and an inter-session one, where enrollment and test are performed on different days. The resulting benchmarks and processed data are made public, allowing the reproducibility of the key results obtained based on the provided score files and scripts. In addition to remarkable performance thanks to the proposed orientation-based conditional processing, the results show various new insights into the distinctiveness of swipe interaction, e.g.: some gestures hold more user-discriminate information, data from landscape orientation is more stable, and horizontal gestures are more discriminative in general than vertical ones.

Project Title:

Preprocessing and Feature Selection for Improved Sensor Interoperability in On-Line Biometric Signature Verification

Author Name:

RUBEN TOLOSANA, RUBEN VERA-RODRIGUEZ,, JAVIER ORTEGA-GARCIA, JULIAN FIERREZ

ABSTRACT

Due to the technological evolution and the increasing popularity of smart phones, people can access an application using authentication based on biometric approaches from many different devices. Device interoperability is a very challenging problem for biometrics, which needs to be further studied. In this paper, we focus on interoperability device compensation for online signature verification since this biometric trait is gaining a significant interest in banking and commercial sector in the last years. The proposed approach is based on two main stages. The first one is a preprocessing stage where data acquired from different devices are processed in order to normalize the signals in similar ranges. The second one is based on feature selection taking into account the device interoperability case, in order to select to select features which are robust in these conditions. This proposed approach has been successfully applied in a similar way to two common system approaches in online signature verification, i.e., a global features-based system and a time functions-based system. Experiments are carried out using Biosecure DS2 (Wacom device) and DS3 (Personal Digital Assistant mobile device) dynamic signature data sets which take into account multisession and two different scenarios emulating real operation conditions. The performance of the proposed global features-based and time functions-based systems applying the two main stages considered in this paper have provided an average relative improvement of performance of 60.3% and 26.5% Equal Error Rate (EER), respectively, for random forgeries cases, compared with baseline systems. Finally, a fusion of the proposed systems has achieved a further significant improvement for the device interoperability problem, especially for skilled forgeries. In this case, the proposed fusion system has achieved an average relative improvement of 27.7% EER compared with the best performance of time

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006234|

functions-based system. These results prove the robustness of the proposed approach and open the door for future works using devices as smart phones or tablets, commonly used nowadays.

III. PROPOSED METHODOLOGY AND DISCUSSION

EXISTING SYSTEM

In existing system handwritten signature is one of the most socially accepted biometrics as it has been used in financial and legal agreements for many years and it also finds applications in mobile scenarios. These approaches are based on the combination of two authentication stages. The security system checks that the claimed user introduces its unique password correctly, and its behavioral biometric information is used for an enhanced final verification. The software for capturing handwritten numerical digits was developed in order to minimize the variability of the user during the acquisition process. The selection of a password that is robust enough for a specific application is a key factor. The number of digits that comprise the password depends on the scenario and level of security considered in the final application.
This effect has proven to be very important for many behavioral biometric traits such as the case of the handwritten signature.

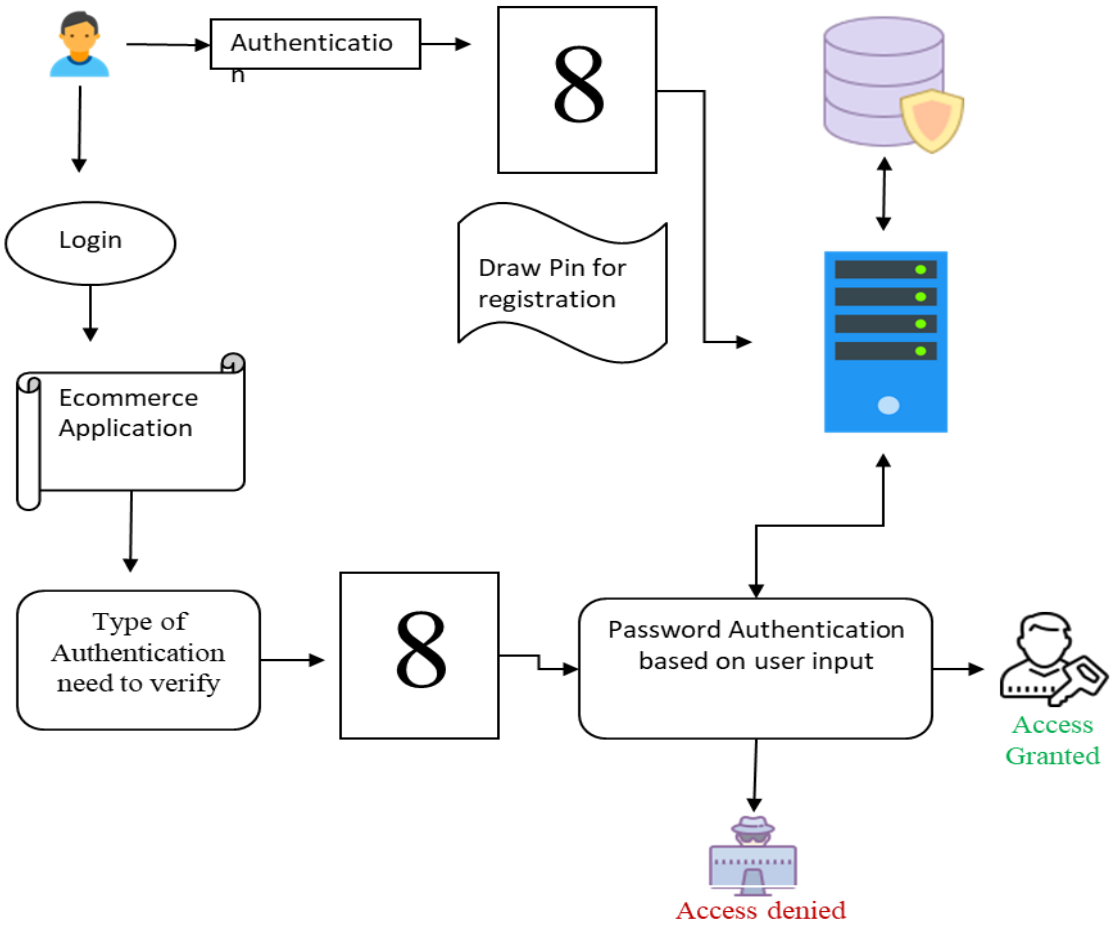
PROPOSED SYSTEM: Our proposed system focus on providing user-friendly mobile applications ensuring data protection and high security. User should draw each digit of the password on the touch screen instead of typing them as usual. This way, the traditional authentication systems are enhanced by incorporating dynamic handwritten biometric information. Our system involves two stages of authentication the drawn pin should be similar to pin entered during registration process.
Our second stage of authentication involves multiple options based on user preference where user can set multiple set of combinations. User can set 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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006234|

ARCHITECTURE DIAGRAM:



IV. 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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006234|

[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 Smart Phones," 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 Passwordbased 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.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details