Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 11, November -2016

Enhancing Privacy and Security by Visual Authentication System and QR Code Strategy

Apurva Maloo[1], Sneha Patil[2] , Jagruti Mhetre[3], Mrinal Mathesul[4], Prof. S. S. Raskar[5]

[1,2,3,4,5] *Department of Computer Engg, Modern Education Society's College Of Engg, Pune,*

Abstract — *Keylogging or keyboard capturing is that the activity of recording (or logging) the keys smitten on a keyboard, Usually during a close lipped manner so the individual utilizing the keyboard is unconscious that their activities are being discovered. It likewise has exceptionally authentic uses in investigations of human-computer interaction. There are varied Keylogging techniques, extending from hardware and computer code based mostly methodologies to acoustic examination. as well as human in authentication protocols, whereas guaranteeing, isn't easy in light-weight of their restricted capability of calculation and remembrance. The project exhibits however careful mental image define will improve the safety likewise because the convenience of authentication. The system propose 2 visual authentication protocols: one may be a one-time-password protocol, and therefore the different may be a password-based authentication protocol. Our approach for real arrangement: the system has the capability attain to associate abnormal state of simple use whereas fulfilling rigorous security requirements.*

Keywords- *Authentication, smartphone, malicious code, keylogger*

I. INTRODUCTION

Hospital are terribly essential a part of our lives, providing best medical facilities to folks full of numerous diseases. However keeping track of all the activities and records is extremely error prone. It's conjointly terribly inefficient and time intense method perceptive the continual increasing population and range of individuals visiting the hospital. Recording and maintaining the record is extremely unreliable and error prone and inefficient. It's conjointly not economically and technically possible to take care of the records on paper. The most aim of project is to supply paper-less up to ninetieth. It conjointly aims at providing low value reliable automation of the present system. There are numerous Keylogging techniques, extending from hardware and computer code based mostly methodologies to acoustic examination. Together with human in authentication protocols, whereas guaranteeing, isn't straightforward in lightweight of their restricted capability of calculation and remembrance. Fast Response (QR) codes appear to look everyplace lately. victimization the QR codes is one amongst the foremost intriguing ways in which of digitally connecting shoppers to the web via mobile phones since the mobile phones became a basic necessity issue of everybody. For making QR codes, the admin can enter text into an internet browser and can get the QR code generated. Whereas QR codes have several benefits that create them very hip, there are many security problems and risks that are related to them. Running malicious code, stealing users' sensitive data and violating their privacy and fraud are some typical security risks that a user could be subject to within the background whereas he/she is simply reading the QR code within the foreground. A security system for QR codes that guarantees each users and generators security considerations are going to be enforced. The project exhibits however careful visualization define will improve the safety further because the convenience of authentication. Because of increase in range of road accidents there's a requirement to access a person's medical/contact data just in case of emergencies for care and hospital & alternative formalities. So as to shorten the admitting procedures once a patient seen within the emergency department is afterward admitted to the hospital, we are going to be retrieving their data keep in cloud information that is scanned with the assistance of a QR Code containing a link to the victim's emergency data. This can facilitate hospital authority to relinquish acceptable medication to the accident victim and inform his/her family.

In order to shorten the admitting procedures once a patient seen within the emergency department is afterward admitted to the hospital, we are going to be retrieving their data that is scanned with the assistance of a QR Code containing a link of the victim's emergency data keep in cloud information. Initially, the user has to feed his data into

the information. Then, we are going to generate a second dynamic QR Code with the assistance of a novel address. This second dynamic QR Code are going to be provided to the users within the type of a wise card.

II.LITERATURE SURVEY

1. Paper Name: Panorama: Capturing System-Wide Information Flow for Malware Detection and Analysis.

Authors: Heng Yin, Dawn Song,Manuel Egele, Christopher Kruegel, Engin Kirda

Description: Malicious programs spy on users' behavior and compromise their privacy. Even code from respectable vendors, like Google Desktop and Sony DRM media player, might perform undesirable actions. Sadly, existing techniques for detection malware and analyzing unknown code samples square measure scarce and have vital shortcomings. we have a tendency to observe that malicious data access and process behavior is that the elementary attribute of diverse malware classes breaching users' privacy (including keyloggers, countersign thieves, network sniffers, concealing backdoors, spyware and rootkits), that separates these malicious applications from benign code. we have a tendency to propose a system, Panorama, to discover and analyze malware by capturing this elementary attribute. In our intensive experiments, Panorama with success detected all the malware samples and had only a few false positives. what is more, by exploitation Google Desktop as a case study, we have a tendency to show that our system will accurately capture its data access and process behavior, and that we will make sure that it will remit sensitive data to remote servers in bound settings[11].

2. Paper Name: Reducing Shoulder-surfing by Using Gaze-based Password Entry.

Authors: Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd

Description: Shoulder-surfing mistreatment direct observation techniques, like wanting over someone's shoulder, to induce passwords, PINs and different sensitive personal info could be a downside that has been troublesome to beat. Once a user enters info employing a keyboard, mouse, bit screen or any ancient device, a malicious observer could also be able to acquire the user's word credentials. we have a tendency to gift Eye Password, a system that mitigates the problems of shoulder aquatics via a unique approach to user input. With Eye Password, a user enters sensitive input (password, PIN,etc.) by choosing from Associate in Nursing on-screen keyboard mistreatment solely the orientation of their pupils (i.e. the position of their gaze on screen), creating eavesdropping by a malicious observer mostly impractical. We have a tendency to gift variety of style decisions and discuss their result on usability and security[6].

3. Paper Name: Vigilare: Toward Snoop-based Kernel Integrity Monitor.

Authors: Hyungon Moon,Hojoon LeeJihoon , LeeKihwan Kim, Yunheung Paek
Brent Byunghoon Kang

Description: In this paper, authors gift Vigilare system, a kernel integrity monitor that's architected to snoop the vehicular traffic of the host system from a separate freelance hardware. This snoop-based observation enabled by the Vigilare system, overcomes the restrictions of the snapshot-based observation used in previous kernel integrity observation solutions. Being supported inspecting snapshots collected over a particular interval, the previous hardware-based observation solutions cannot discover transient attacks which will occur in between snapshots. We tend to enforced a image of the Vigilare system on Gaisler's grlib-based system-on-a-chip (SoC) by adding spy hardware connections module to the host system for bus snooping. To guage the good thing about snoop based mostly observation, we tend to conjointly enforced similar SoC with a snapshot-based monitor to be compared with[8].

4. Paper Name: Short Signatures Without Random Oracles.

Authors: Dan Boneh, Xavier Boyen

Description: Here authors describe a brief signature theme that is existentially unforgeable below a selected message attack while not victimization random oracles. The protection of our theme depends on a brand new quality assumption we tend to decision the robust Diffie-Hellman assumption. This assumption has similar properties to the robust RSA assumption, thence the name. Robust RSA was antecedently wont to construct signature schemes while not random oracles. However, signatures generated by our theme area unit a lot of shorter and less complicated than signatures from schemes supported robust RSA. Moreover, our theme provides a restricted kind of message recovery[13].

5. Paper Name: YAGP: Yet Another Graphical Password Strategy.

Authors: Haichang Gao, Xuewu Guo, Xiaoping Chen, Liming Wang, and Xiyang Liu

Description: Alphanumeric passwords are wide utilized in pc and network authentication to guard user's privacy. However, it's documented that long, text based mostly passwords are arduous for folks to recollect, while shorter ones are at risk of attack. Graphical watchword may be a promising answer to the present drawback. Draw-A-Secret (DAS) may be a typical implementation supported the user drawing on a grid canvas. Currently, too several constraints lead to reduction in user expertise and forestall its quality. a completely unique graphical watchword strategy yet one more Graphical watchword (YAGP) galvanized by DAS is projected during this paper. The proposal has the benefits of free drawing positions, robust shoulder water sport resistance and huge watchword area. Experiments illustrate the effectiveness of YAGP [12].

III.PROPOSED SYSTEM

In order to shorten the paperless work procedures once a patient visiting often or seen within the emergency case, we'll be retrieving their data that is scanned with the assistance of a QR Code containing a link of the victim's emergency data keep in info.

When patients 1st visits to hospital, perform registration method with system. At the time of login there are a unit 2 the 1st step is positive identification based mostly} and another is OTP based, in positive identification based mostly he can enters the his username/ email with positive identification. In second step the system can raise the OTP displayed the traditional input device that is unreal and revered OTP and therefore the actual pattern of that input device is distributed to users email ID upon with success coming into the right email and positive identification of that user. Upon thriving login, user can his check up details and submits and system can generate the QR of that users data which QR are going to be keep at admins records and user can get the ID for his record. Once user visits the hospital he can tell solely his ID and admin can scan respected ID's QR code and issue consequently.

If any amendment in users details then he can login to his account and do changes then system can generate new QR code. And next time admin can use that new generated QR code. The admin or hospital one that handling this method will read all the small print of all the users registered therewith system as he's solely licensed person.

IV.SYSTEM ARCHITECTURE

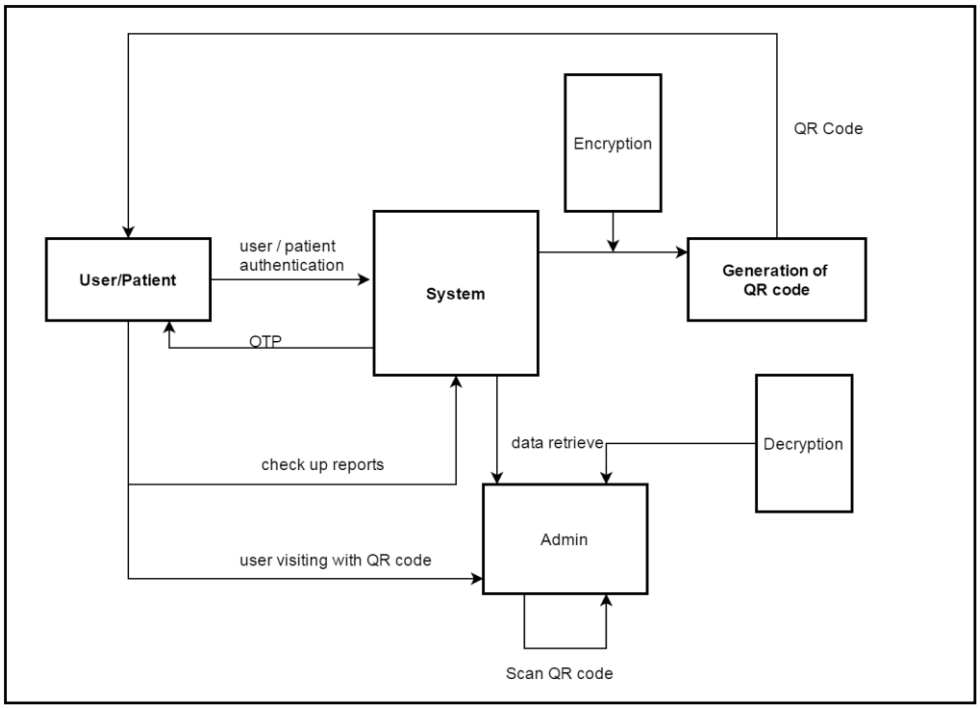

Fig.1 System Architecture

Step-1: Registration Process.

In this stage, the user will fill an online form provided by the organization on their website.
This online form will be consisting of all required details for the database.
Information stored in database and displayed to user. After successfully filling the online form, the information will be stored in the database and the webpage which will contain all the details of the user will be shown to the user. The database will be stored in the cloud.

Step-2: Generate QR code
After successful registration of user the QR code is generated by the system.
Using the unique URL generated for the webpage of each user, unique 2D QR code will be generated for each user.

Step-3: Sending confirmation mail containing the QR code to the user.
A confirmation mail containing the unique 2D QR code and secrete key which is used to decrypt that QR code of the user will be sent to the user after the QR code is generated successfully.

Step-4: Scan QR code
A smartphone application will be used for scanning the QR code. Before scanning the QR code, authorized login will be provided to the particular authorities like police, hospital management, or admin and the user itself.

Step-5: Link retrieval and display link
After scanning the QR code, a link will be retrieved and displayed to the user scanning the QR code.

Step-6: Display information of the victim/user
After displaying the link, the user have to click on the link and then the webpage or a page consisting of that user's details will be displayed.

V. CONCLUSION AND FUTURE SCOPE

We projected and analyzed the utilization of user driven visual image to enhance security and user-friendliness of authentication approaches. Projected 2 of conventions that not solely improve the user expertise however additionally resist difficult attacks, like the keylogger and malware attacks. Our protocols utilize straightforward technologies on the market in most out-of-the box Smartphone devices.

ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

REFERENCES

1. R.Pemmaraju Methods and apparatus for securing keystrokes from being intercepted between the keyboard and a browser. Patent 182,714.
2. N. Hopper and M. Blum. Secure human identification protocols. In *Proc. of ASIACRYPT*, 2001
3. DaeHunNyang, Member, IEEE, Aziz Mohaisen, Member, IEEE, Jeonil Kang, Member, IEEE, "**Keylogging-resistant Visual Authentication Protocols**" -IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 11, NOVEMBER 2014
4. J. Bonneau, C. Herley, P.C. Van Oorschot, and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," Proc. IEEE Symp. Security and Privacy (SP), pp. 553-567, 2012.
5. M. Farb, M. Burman, G. Chandok, and J. McCune, "A. Perrig, "SafeSlinger: An Easy-to-Use and Secure Approach for Human Trust Establishment," Technical Report CMU- CyLab-11-021, Carnegie Mellon Univ., 2011.
6. M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing Shoulder-Surfing by Using Gaze-Based Password Entry," Proc. ACM Third Symp. Usable Privacy and Security (SOUPS), pp. 13-19, 2007.
7. M. Mannan and P.C. van Oorschot, "Leveraging Personal Devices for Stronger Password Authentication from Untrusted Computers," J. Computer Security, vol. 19, no. 4, pp. 703-750, 2011.
8. H. Moon, H. Lee, J. Lee, K. Kim, Y. Paek, and B.B. Kang, "Vigilare: Toward Snoop-Based Kernel Integrity Monitor," Proc. ACM Conf. Computer and Comm. Security (CCS '12), pp. 28-37, 2012.
9. D. MRaihi, S. Machani, M. Pei, and J. Rydell, "TOTP: Time-Based One-Time Password Algorithm," RFC 6238, http://www.ietf. org/rfc/rfc6238.txt, 2011.
10. Q. Yan, J. Han, Y. Li, J. Zhou, and R.H. Deng, "Designing Leakage- Resilient Password Entry on Touchscreen Mobile Devices," Proc. Eighth ACM SIGSAC Symp. Information, Computer and Comm. Security (ASIACCS), pp. 37-48, 2013.
11. H. Yin, D. Song, M. Egele, C. Kruegel, and E. Kirda, "Panorama: Capturing System-Wide Information Flow for Malware Detection and Analysis," Proc. ACM Conf. Computer and Comm. Security (CCS), 2007.
12. H. Gao, X. Guo, X. Chen, L. Wang, and X. Liu, "YAGP: Yet Another Graphical Password Strategy," Proc. ACM Ann. Computer Security Applications Conf. (ACSAC), pp. 121-129, 2008.
13. D. Boneh and X. Boyen, "Short Signatures without Random Oracles," Proc. Advances in Cryptology (EUROCRYPT), pp. 56-73, 2004.

