Scientific Journal of Impact Factor (SJIF): 4.72

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

International Journal of Advance Engineering and Research Development

Volume 4, Issue 12, December -2017

Social Engineering: E-Documents with Applied QR-code & Keylogging Security

Nikhil Tekawade[1], Shruti Kshirsagar [2], Shripad Sukate[3], Prof. Leena Raut[4]

[1,2,3,4]*Department of Computer Engineering, Siddhant College of Engineering, Pune.*

Abstract — *In this era of technology driven management why would you want to physically manage your documents. the merits of electronic documentation are countless, saves up your time ,money ,resources and increased security of documents. User is able to manage documents digitally such that information can be shared ,created, retrieved, organized and stored efficiently and appropriately. As user requires to obtain some government certificates for general needs or every year , the current process of obtaining a certificate or document is lengthy. This system can generate retrieve certificates and documents through e-documents. Security techniques used are QR code and keylogging . QR code is 2D matrix code that is designed by keeping two point under consideration, i.e. it stores large amount of data as compared to 1D barcodes . Security is mainly focused on keylogging where the keylogger hardware or software is used to capture the client's keyboard strokes to intercept the password. One Time Password(OTP) system is a secure implementation and designed to for providing a stricter set of policies depart from natural human habits of choosing their own passwords does not endure by functionalities of an organization , leaving unsafe from different malicious attacks.*

Keywords- *Design, Human factors, Unauthorized access, Security, Graphical passwords, Social engineering, Distortion.*

I. INTRODUCTION

The THREATS against electronic and financial services can be classified into two major classes: channel breaking attacks and credential stealing. Credentials such as users identifiers, passwords, and keys can be stolen by an attacker when they are poorly managed. For example, a poorly managed personal computer (PC) infected with a malicious software (malware) is an easy target for credential attackers, On the other hand, channel breaking attacks which allow for eavesdropping on communication between users and a financial institution are another form of exploitation. While classical channel breaking attacks can be prevented by the proper usage of a security channel such as IPSec and secure sockets layer (SSL) , recent channel breaking attacks are more challenging. Indeed, keylogging attacks or those that utilize session hijacking, phishing and pharming, and visual fraudulence can-not be addressed by simply enabling encryption. Chief among this class of attacks are keyloggers A keylogger is a software designed to capture all of a users keyboard strokes, and then make use of them to impersonate a user in financial transactions. For example, whenever a user types in her password in a banks sign-in box, the keylogger intercepts the password. The threat of such keyloggers is pervasive and can be present both in personal computers and public kiosks; there are always cases where it is necessary to perform financial transactions using a public computer although the biggest concern is that a users password is likely to be stolen in these computers. Even worse, keyloggers, often rootkitted, are hard to detect since they will not show up in the task manager process list. To diminish the keylogger attack, virtual or onscreen keyboards with random keyboard arrangements are broadly used in practice. Both techniques, can frustrate simple keyloggers, by rearranging alphabets randomly on the buttons. Unfortunately, the keylogger, which has control over the entire PC, can easily capture every event and read the video buffer to create a mapping between the clicks and the new alphabet. Another mitigation technique is to use the key board hooking prevention technique by perturbing the keyboard interrupt vector table . However, this technique is not universal and can interfere with the operating system and native drivers.

II. LITERATURE SURVEY

1. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes (2012)
Author: Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajanoy.

Description:
For general-purpose user authentication on the web using a broad set of twenty-five usability, security benefits and deployability that an ideal scheme might provide, authors have been evaluated two decades of proposals to replace text passwords. The scope of proposals their survey is also extensive, including one-time passwords, cognitive authentication schemes, graphical password schemes, federated login protocols , password management software, biometrics, phone-aided schemes and hardware tokens. Authors inclusive approach leads to key intuition about the difficulty of replacing passwords. The scheme is not only providing all desired benefits but also not retains the full set of required legacy passwords already provided. In particular, there is a wide range from schemes offering significant security benefits in return for being more costly to deploy or more difficult to use, to those offering minor security benefits beyond legacy

passwords. Authors conclude that because of researchers rarely consider a sufficiently broad range of real-world limitations many academic proposals have failed to gain adhesion. Beyond authors analysis of current schemes, their framework provides an evaluation methodology and benchmark for future web authentication proposals.

2.SafeSlinger: Easy-to-Use and Secure Public-Key Exchange (2011)
Author: MFarb, Yue-Hsun Lin, Tiffany Hyun-Jin Kim, Jonathan McCune, A Perrig

Description:
Users regularly get known about thelack of confidence on the Internet. Is that email or instant message truly originating from the claimed individual? Such doubts are commonly resolved through a bound of faith, expressing the state of dispair and helplessness of users. To establish a secure basis for online communication, authors propose Safe-Slinger, a system dominance the growth of smartphones to enable people to securely and privately exchange their public keys. Through the interchanging authentic public keys, Safe-Slinger establishes a secure path channel contributing secrecy and authenticity, which authors use to support secure messaging and exchanging a file. Safe-Slinger also provides an Application programming interface for importing applications public keys into a users contact information. By suspending entire contact entries to others, they propose secure introductions, as the contact entry includes the Safe-Slinger public keys as well as other public keys that were imported.

3.Leveraging Personal Devices for Stronger Password Authentication (2011).
Author: Mohammad Mannan and P.C. van Oorschot

Description:
End user transactions such as online banking E-commerce continues to be influenced by passwords entered through end user's PC's. Internet authentication has dominated use for online internet transaction. The underlying protocols of most of the transactions exposed to the possibility of being attacked of harmed by susceptible attacks including keylogging phishing and pharming. Authors suggest Mobile Password Authentication (MP-AUTH) for retaliation of such attack and offers transaction integrity. Password authentication separates a users long standing secret input from client PC. PC has ingress to only temporary secrets and continues to be used for most of the transactions. long term secret is input through a personal device which makes it available to the PC under the recipients public key after encryption. MP-AUTH look ahead users to input passwords only to personal device and be attentive while assuring transactions from device. They also provide wide ranging survey to facilitate a comparison to MP-AUTH of web authentication techniques that use additional factor of authentication.

4.An Introduction To QR Code Technology(2016).
Author: Sumit Tiwari

Description :
“Quick Response” code called as QR code is a 2D matrix code which keeps two points under consideration ,firstly it must be designed to store large amount of data as compared to 1D barcodes and its decoded speed should be high using any handheld devices like phones. Initially these codes where used for tracking inventry in vehical parts manufacturing. QR codes provides omni directional readability, and various advantages including , high level error correction , up to 30% of the image can be smudged and still be recognized. L, M, Q or H are defined as levels of error correction.(H) makes higher level notable correction which makes the code uncomplicated and effortless to scan. (L) is low amount of error correction which allows more content to be added in the QR code . The code consist of black modules arranged in a square pattern on a white background which can be read by an imaging device such as a camera, and processed using Reed–Solomon error correction until the image can be appropriately interpreted. The QR code can store up to 4,296 alphanumeric or 7,089 numeric characters. Different varieties of QR code symbols like logo QR code, encrypted QR code, iQR Code are also available so that user can choose among them according to their need. By using QR code generating sites or apps, users can generate and print their own QR codes for others to scan and use. The idea behind the development of the QR code is the limitation of the barcode information capacity (can only hold 20 alphanumeric characters). The popularity of QR codes is growing rapidly all around the world.

III. EXISTING SYSTEM

It is a system where user can apply for the document. It include the application forms as per the user want to apply for the particular document. The security applied is the captcha system to check whether the applicant is a robot or a human being. Whenever the user type in the password in the system's login the keylogger intercepts the password. The threat of such keyloggers can be present in both personal as well as public kiosks. As there are always cases using public computer where the biggest threat is that the password is likely to be stolen in this computers. Also the application from the user can be manipulated or changed as there is no any encryption or decryption process.

Moreover a secured and authentication based application process is needed. Prior works have elaborated on applying for document.

Disadvantages :

- No security of documents.
- No security for the applications applied by user.
- No secured authentication.
- Time consuming system.
- Is not an user friendly system.

IV. PROPOSE SYSTEM

In this proposed system an secure and reliable system for e-documents is being developed. In this system first the user have to get registered on the web portal and then he will able to avail different services provided by the system. System provides an interactive user interface.

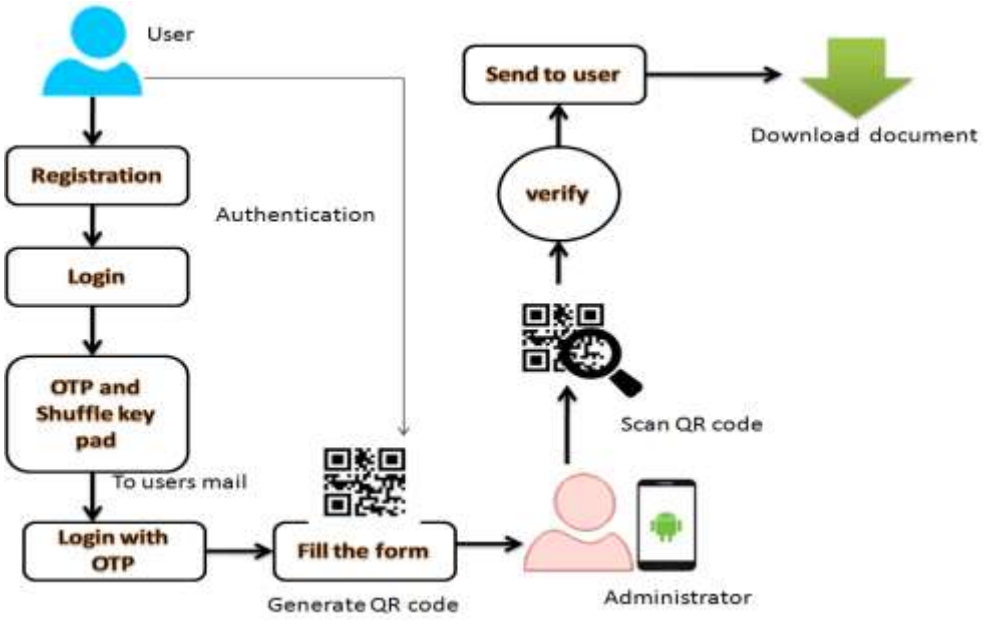

Figure 1. System Architecture

User have to login. While logging in the user will get an OTP through email or message. To avoid keylogging user have to enter OTP/password through shuffle keyboard. By logging in to the portal the user choose the documents which he wanted to retrieve and he have to fill the required details in the form. The form is encrypted and hidden behind the QR code. The QR code is send to the user and the respective third party. The third party can scan and decrypt the QR code by an specially designed app only. The third party have an user id and password by using that the party can log in to app and do further work. The third party will verify and issue the documents required to the user on his respective email id. The third party will verify and keep them in their database and an reference number will be given to the user. Then next time when if user again wanted to retrieve the documents he will only give the reference number with the form.

Advantages :

- Auto filling of data when user is registered in the system.
- Security for documents.
- Retrieval of documents from anywhere.
- Secure authentication.
- Security from various attacks like shoulder surfing attack, bruteforce, credential stealing, keyloggers, channel breaking.

V. MATHEMATICAL MODEL

Let W be the whole system which consists
Input = U, M, C, k, S, M.
Let u is the set of number of users.
U= u1, u2.un.

k is the secret key used for encryption.
M is the message sent from the set M.
C is the cipher-text in the set C
S is the signature generated for sending message.
Functions:
1. QREnc (): a QR encoding algorithm which takes a string S in S and outputs a QR code.
2. QRDec (): a QR decoding algorithm which takes a QR code and returns a string S in S.

VI. SUMMARY AND CONCLUSION

We proposed and analyzed the use of user driven visualization to improve security and user-friendliness of authentication approaches. Proposed two of conventions that not only improve the user experience but also resist challenging attacks, such as the keylogger and malware attacks. Our protocols utilize simple technologies available in most out-of-the box Smartphone devices.

REFERENCES

[1] C. Saiprasert , W. Pattara-Atikom, "Smartphone enabled dangerous driving report system", in Proc. HICSS, 2013, pp.12311237.

[2] S. Al-Sultan, A. H.Al-Bayatti, and H. Zedan, "Context-aware driver behavior detection system in intelligent transportaion system", IEEE Trans. on Vehicular Technology, vol. 62, pp. 42644275, 2013.

[3] Lara-Ni˜no, Carlos Andr´es, Morales-Sandoval, Miguel and D´ıaz-P´erez , "An evaluation of AES and PRESENT ciphers for lightweight cryptography on smartphones", 2016 IEEE.

[4] J. Paefgen, F. Kehr, Y. Zhai, and F. Michahelles, "Driving behavioral analysis with smartphones: insights from a controlled field study".2012

[5] H. Han, J. Yu, H. Zhu, Y. Chen, J. Yang, Y. Zhu, G. Xue, and M. Li, "Senspeed: Sensing driving conditions to estimate vehicle speed in urban environments", inProc. IEEE INFOCOM , 2014.

[6] Swapnoneel Roy, Matt Rutherford, Charlene H. Crawshaw "Towards Designing and Implementing a Secure One Time Password (OTP)Authentication System", 2016 IEEE.

[7] S. Reddy, M. Mun, J. Burke, D. Estrin, M. Hansen, and M. Sri-vastava, "Using mobile phones to determine transportation modes",ACM Trans. on Sensor Networks vol. 6, no. 13, 2010.

[8] M. Fazeen, B. Gozick, R. Dantu, M. Bhukuiya, and M. C.Gonzalez, "Safe driving using mobile phones" ,IEEE Trans. on Intelligent Transportation Systems vol. 13, pp. 14621468, 2012.

[9] D. Lee, S. Oh, S. Heo, and M. Hahn, "Drowsy driving detectionbased on the drivers head movement using infrared sensors", in Proc. IEEE ISUC , 2008, pp. 231236.

