Smart-Authentication: A secure web service for providing bus pass renewal system

Priyanka Bhunde[1], Rutuja Pol[2], Trupti Chandgude[3],Shambhavi Nangare[4] ,Prof. Shrikant Nagure[5]

[1]Priyanka Bhunde, Dept. of Computer Engineering, RMD Sinhgad School of Engineering, Maharashtra, India
[2]Rutuja Pol, Dept. of Computer Engineering, RMD Sinhgad School of Engineering, Maharashtra, India
[3]Trupti Chandgude, Dept. of Computer Engineering, RMD Sinhgad School of Engineering, Maharashtra, India
[4]Shambhavi Nangare, Dept. of Computer Engineering, RMD Sinhgad School of Engineering, Maharashtra, India
[5]Professor Shrikant Nagure, Dept. of Computer Engineering, RMD Sinhgad School of Engineering, Maharashtra, India

---***---

Abstract - *Now a day we are towards the development of smart city, so all people want everything on their finger tips and there has been also increase in use of mobile devices like smart phones and tablets. Web has become the dominant interface for people to conduct their daily businesses on the Internet or a corporate network. People use their PCs to check email, access financial accounts, to do online shopping, all through a web browser. In this paper We are developing an application for bus pass renewal and we are providing Web security using Smart-Authentication, a web authentication scheme that exploits pervasive mobile devices and digital cameras to counter various password attacks including man-in-the-middle and phishing attacks. In Smart-Authentication, a mobile device is used as the second authentication factor to vouch for the identity of a use that is performing a web login from a PC.*

Smart-Authentication employs public key cryptography to ensure the Security of authentication process. We implemented a prototype system of Smart-Authentication that consists of an Android application, a Chrome browser extension, and a Java-based web server.

Key Words: **: QR-Code or Barcode, Visible Light Communication (VLC),Phishing attack,Cryptography web server,TFA(Two Factor Authentication).**

1.INTRODUCTION

In several areas and particularly in business, Web has become the dominant interface for people to conduct their daily businesses on the web or company network authentication .In general, a user authenticates herself to an internet application hosted on a remote server by coming into her username and positive identification in the application's login page (either manually or mechanically through a positive

identification manager). positive identification has been the First State facto methodology for net authentication [1]. However password only authentication cannot give ample cannot give ample protection because the mechanism is at risk

Of a range of attacks together with shoulder surfing attack [2] To improve net authentication security and facilitate positive identification management, thought net browsers(e.g chrome , Firefox, and net Explorer) have introduced integral positive identification managers Standalone positive identification Managers (e.g., 1Password and KeyPass) and web based positive authentication managers that run during browser.

However, a password manager alone does not provide ample security assurance due to insecure computing environments at either native or remote. Zhao and Cantonese dialect showed that none of the browser integral password managers in thought net browsers may stop malware from stealing passwords during a laptop setting [3]. Recent studies on net on net positive identification automobile filling [11] and web based password managers [4] reveal that there exist variety of Serious vulnerabilities in standard positive identification Managers.

In recent years we have observed that frequent happening of knowledge breaches and positive identification info leaks that occurred on outstanding websites similar to LinkedIn , Yahoo! and Gmail .Those positive identification leaks endanger countless people's data security not solely on those websites however additionally on alternative websites thanks to positive identification employ to create matters worse, attackers usually launch MITM attack and phishing attack to steal users' passwords. The recent MITM attack against Iranian Google users demonstrates that even a user of well maintained and hardened web site may be subjected to the MIMM attack.

Camauth consist of an android application ,a chrome browser extension,and a java-based web server .The main of this project to assure the security of web security while renew a pass ,it is very cost effective and convenient to the user .This system is made as user friendly as possible so that anyone can use it with little knowledge of system computers.

2. LITERATURE SURVEY

We first evaluate CamAuth using the web authentication assessment framework proposed by Bonneau *et al.* [1]. We compare e CamAuth with passwords, a most popular TFA scheme—Google 2-step verification (2SV) [6], and a relevant mobile device based TFA scheme—PhoneAuth (in strict mode) [7].A barcode scanning using smartphone is already widely used, we grant *Easy-to-Learn* and quasi *Easy-to-Use* to CamAuth according to the definition of those benefits [1]. We believe that CamAuth (barcode scanning as user action) is easier to use than 2SV (PIN typing as user action) even though both have the same rating. We grant quasi *Infrequent-Errors* to CamAuth, the same as all others, as barcode scanning from either smartphone or PC is fairly accurate and the camera performance keeps improving.

3. BACKGROUND

Two-factor authentication (TFA) requires the presentation of two or more authentication factors: something a user knows (e.g., a password), something a user has (e.g., a secure token), and something a user is (e.g., biometric characteristics) In this paper we are developing an application for bus pass renewal and we are providing Web security using Smart- Authentication, a web authentication scheme that exploits pervasive mobile devices and digital cameras to counter various password attacks including man-in-the-middle and phishing attacks.

In Smart-Authentication, a mobile device is used as the second authentication factor to vouch for the identity of a use that is performing a web login from a PC. Smart Authentication employs public key cryptography to ensure the security of authentication process. We implemented a prototype system of Smart-Authentication that consists of an Android application, a Chrome browser extension, and a Java-based web server. Recently camerabased communications have attracted much attention given the increasing popularity of mobile devices with one or more built-in cameras. Barcode scanning is the primary application domain of camera-based communications. A barcode is an optical machine-readable representation of information.

There are two types of barcodes: one dimensional (1D) barcodes and two dimensional (2D) barcodes. Quick Response code (QR code) is a popular 2D barcode. All major Smartphone platforms support QR code scanning either natively or through third-party applications. As camera-based communications are short-range, highly directional, fully observational, and immune to electromagnetic interference, they have been applied to security applications. There are four main modules in project are as follows:

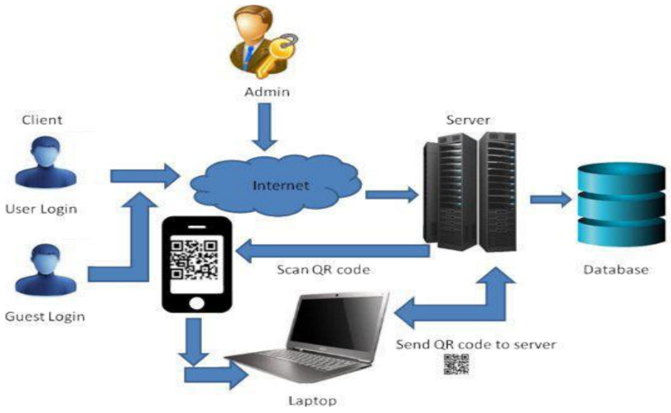

Fig -3.1: System architecture of bus pass system using web server.

A. User registration:

User registration is used for KYC(know your customer) in which you have to upload your documents like photo, aadhar card and enroll your mobile number and set your userid and password according to your wish.

B. User authentication:

In this phase user has to enter his userid and password if it is correct then it will go ahead and ask for your aadhar card no, mobile number etc it will scrutinize all details with the details which are stored in the database.

C. CamAuth registration:

In this phase, barcode i.e QR code is generated and then it is send to laptop through which transcation is going on and then QRcode is also send to registered mobile number of the respective user.

D .Camauth Authentication:

In this phase QRcode which is received on registered mobile number is scanned by laptop's webcam through the secure visible light communication channel. If QRcode match's then it will proceed further. Then user will get choice to choose his rout and other things related to bus pass. But the QRcode which will be generated will be having time session if user doesn't enter QRcode within that time then it will get timed out.

4. SUMMARY

Web authentication is the main part of camauth. we presented a secure bus pass renewal system using CamAuth.The online bus pass system will help to get a bus passes online and reduce Endeavour. User can obtain all bus related information through this system.It is camera based TFA scheme that provide security of web login.

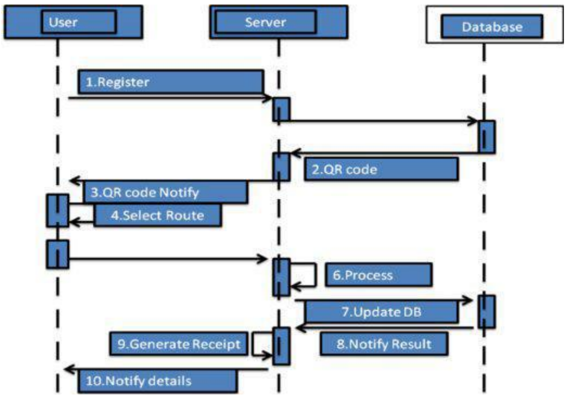

Fig -4.1: Activity diagram

5. CONCLUSION

In this paper we presented a secure bus pass renewal system using CamAuth, a camera based TFA scheme that augments the security of web login from PC. Leveraging the high market penetration of mobile devices and pervasive barcode scanning through camera, CamAuth realizes two-factor Authentication through passwords plus barcode scanning using user's mobile device. The public-key cryptography and secure visible light communications ensure that CamAuth can effectively defeat password stealing attacks including man-inthe- middle and phishing attacks. CamAuth requires no Modification to existing network protocols and operating system of PC and mobile device. Our viability of the scheme. In future, prototype system and preliminary user study demonstrate the we plan to conduct an extensive usability study to better understand the impact of using barcode scanning for web login on average users physically and psychologically.

6.REFERENCES

[1] CamAuth: Securing Web Authentication with Camera Mengjun Xie ,Yanyan Li , Kenji Yoshigoe , Remzi Seker , Jiang Bian Department of Computer Science University of Arkansas at Little Rock 2015.

[2] M. Mannan and P. van Oorschot, Leveraging personal devices for stronger password authentication from untrusted computers,*Journal of Computer Security*, vol. 19, no. 4, pp. 703–750, 2011

[3] A. Czeskis, M. Dietz, T. Kohno, D. Wallach, and D. Balfanz, "Strengthening user authentication through opportunistic cryptographic identity assertions",in *Proceedings of the 2012 ACM conference on Computer and communications security*, ser. CCS '12, 2012, pp. 404–414.

[4] B. Parno, C. Kuo, and A. Perrig, "Phoolproof phishing Prevention",in Proceedings of the 10th International Conference on Financial Cryptography and Data Security (FC 2006), 2006, pp. 1–19.

[5] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes",in *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, 2012, pp. 553–567.

[6] F. Tari, A. A. Ozok, and S. H. Holden,"A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords", in *Proceedings of the Second Symposium on Usable Privacy and Security*, ser. SOUPS '06, 2006, pp. 56–66.