Review On: A Web Authentication using QR code and Cam: Auth

[1]Gurav Saiprasad A, [2]Madhavi Tejas J., [3]Pasalkar Nikhil K., [4]Prof. D.A.Lokare

Department of Computer Engineering, Zeal College of Engineering & Research, University of Pune.

Abstract-*Increasing of positive identification information leaks and server breaches in recent years, issues of internet authentication highly required. Two-factor authentication, despite being safer and powerfully promoted, has not been wide applied to Internet authentication. Investment the unprecedented quality of each personal mobile devices (e.g. smart phones) and bar code scans through camera, CamAuth tend to explore a replacement horizon within the style house of two-factor authentication. CamAuth is an Internet authentication theme that exploits pervasive mobile devices and digital cameras to counter varied countersign attacks as well as man-in-the-middle and phishing attacks. In CamAuth, a mobile device is employed as second authentication to vouch for the identity of a user log in from a computer. The device communicates directly with the computer through the secure visible radiation communication channels that incurs no cellular price and is proof against frequency attacks. CamAuth employs public key cryptography to confirm the protection of authentication method. Our analysis results indicate that CamAuth could be a viable theme for enhancing the protection of internet authentication.*

Keywords: - OTP, QR-Code, TFA

1. INTRODUCTION

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, pay utilities bills, do online shopping, retrieve electronic health records and so on, all through a web browser. Web authentication stands as the first defense line to secure everyone’s web accounts and online data. In general, a user authenticates herself to a web application hosted on a remote server by entering her username and password in the application’s login page (either manually or automatically through a password manager). Password has been the de facto method for web authentication However, password only authentication cannot provide sufficient protection as the mechanism is prone to a variety of attacks including shoulder
surfing attack , password guessing attack , manin-the-middle (MITM) attack , phishing attack, and so on..

CamAuth uses a mobile device (smartphone or tablet) as the second factor to vouch for the user identity during login. The trusted device directly communicates with the PC through the visible light communication channels (established using camera-display links), which are secure as they are short range, highly directional, fully observational, and immune to radio frequency interference. When applying CamAuth to web login, a user only needs to use her device to snap the barcode (e.g., a QR code) on the webpage and let the PC webcam capture the barcode generated by the mobile app for identity attestation. The use of barcode scans not only simplifies user action and secures information transfer but also makes the user be fully aware of the authentication process. Moreover, CamAuth has the following advantages: 1) The scheme requires no Internet connection for the mobile device during authentication. Therefore, it incurs no cost for the communications with the device. 2) The entire scheme is implemented at the application layer. There is no requirement to modify either the PC’s operating system (OS) or the device’s OS or firmware. 3) The scheme does not rely on SSL/TLS although the use of SSL/TLS can further enhance the security.

2. SYSTEM DESIGN

CamAuth is aimed to assure the security of web authentication through a PC web browser in a cost-effective and convenient manner. CamAuth uses a mobile device as the trustworthy second authentication factor. During the CamAuth authentication, the device is used to vouch for the user’s identity. Neither cellular network nor radio frequency (RF) wireless network (e.g., WiFi and Bluetooth) is used for transferring the device's vouch, which avoids various RF attacks. Instead, CamAuth applies visible light communication (VLC) through camera to take advantage of the security and convenience offered by VLC.

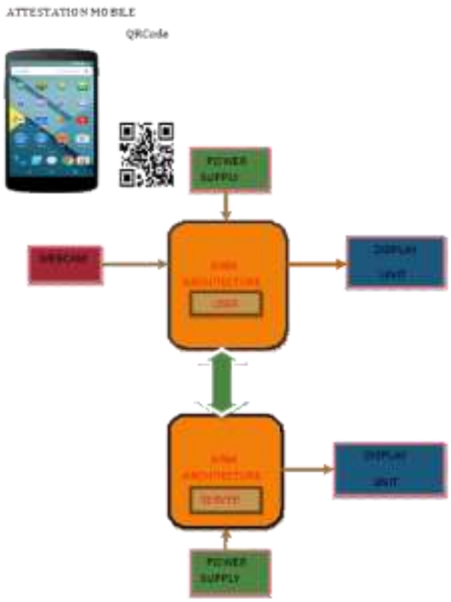

Fig1 System Architecture

Fig: 1 depicts a normal authentication process through CamAuth. The process consists of four interactions between involved entities (i.e., user, PC, mobile device, and web server[1]).

1) A user performs a web login through a web browser by entering her username and password either manually or automatically through a password manager on the login webpage.

2) The web browser is activated to send the username and password (or its hash value; pw is used to represent. For presentation purpose, web application and web server are used interchangeably in the paper unless otherwise noted. Either case for illustration purpose) along with a Diffie- Hellman (DH) exchange request including its dynam- ically generated DH public key to the remote server. After validating the password, the server runs the DH algorithm to derive the shared secret, denoted by OT P, and sends back its identity vouch request and its DH public key.

3) The browser first computes the shared secret based on the received message and then encodes the request with the hash value of the shared secret into a barcode and renders it on the webpage. After scanning the barcode, the CamAuth app on the mobile device verifies the request and vouches for the user's identity using public- key cryptography. The vouch message is encoded into another barcode, rendered on the screen, and captured by the PC's webcam.

4) The vouch message is transferred to the server. If the validation of the vouch succeeds, the server will gener- ate an authentication token (usually a session cookie), encrypt the token with the shared secret, and send it back to the browser, which completes the authentication process.

3. RESULTS

Fig2: Home Page

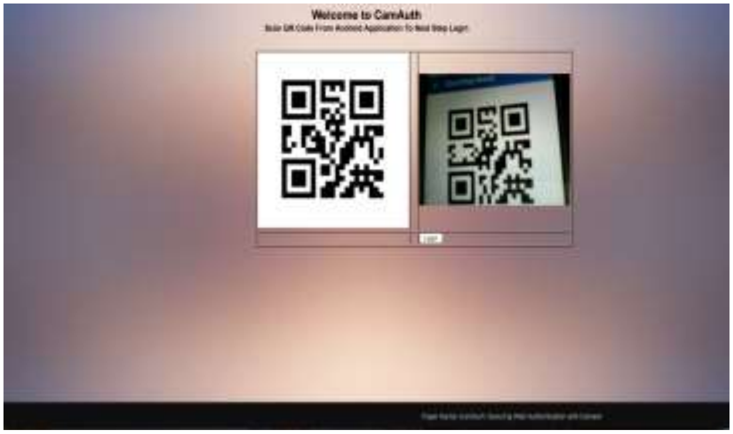

Fig 3: Login With Android Phone

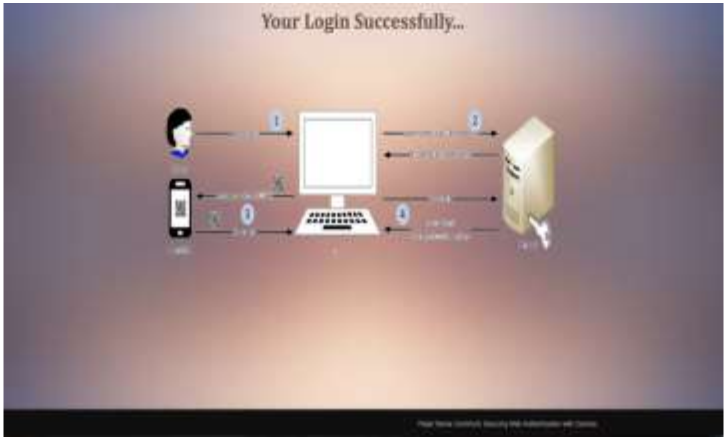

Fig 4: Login Success Page

4. SYSTEM FLOW

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 thenit 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.

5. CONCLUSION

In this paper we propose CamAuth, a camera primarily based TFA theme that augments the safety of net login from laptop. Leverage the high penetration of mobile devices and pervasive barcode scanning through camera, CamAuth realizes two-factor authentication through passwords and barcode scanning mistreatment user's mobile device. The public-key cryptography and secure actinic ray communications make sure that CamAuth will effectively defeat positive identification stealing attacks as well as man-in-the-middle and phishing attacks

REFERENCES

[1] "Mobile-otp: Mobile one time passwords," http://motp.sourceforge.net/.

[2] I. Duo Security, "Duo security: Two-factor authentication made easy," https://www.duosecurity.com/.

[3] Google, "Google 2-step verification," http://www.google.com/landing/ 2step/.

[4] D. Balfanz and E. W. Felten, "Hand-held computers can be better smart cards," in Proceedings of the 8th USENIX Security Symposium, August 1999, pp. 15–24.

[5] 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.

[6] 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.

[7] 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.

[8] J. M. McCune, A. Perrig, and M. K. Reiter, "Seeing-is-believing: Using camera phones for human-verifiable authentication," in Proceedings of the 2005 IEEE Symposium on Security and Privacy, 2005, pp. 110–124.

[9] N. Saxena, J. E. Ekberg, K. Kostiainen, and N. Asokan, "Secure device pairing based on a visual channel: Design and usability study," IEEE Trans. Info. For. Sec., vol. 6, no. 1, pp. 28–38, Mar. 2011.

[10] M. Xie, L. Hao, K. Yoshigoe, and J. Bian, "Camtalk: A bidirectional light communications framework for secure communications on smartphones," in Proceedings of the 9th International Conference on Security and Privacy in Communication Networks (SecureComm'13), 2013, pp. 35–52.