A Web Authentication using QR code and Cam :Auth

[1]Gurav Saiprasad A, [2]Madhavi Tejas J., [3]Pasalkar Nikhil K., [4]Prof. Mr.P.A.Tak

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.*

I. 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 usingcamera-displaylinks),whicharesecureastheyareshortrange, 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 scan 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.

II. RELATED WORK

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). Using two factors as opposed to one factor generally delivers a higher level of authentication assurance. For example, passwords can be combined with security tokens such as RSA SecurID that implement one-time passwords or biometric characteristics suchasfingerprint.Withthepopularityofmobilephone,a new category of TFA tools transforms a PC user's mobile phone into a token device using either SMS messaging [1], an interactive telephone call[2], smartphone application[3]. A number of mobile device-assisted authentication schemes [4], [5], [6], [7] were proposed for protecting a user from either password stealing on an untrusted PC or phishing attacks. In those schemes, mobile devices are assumed to be trustworthy and able to perform certain computing operations such as hashing. Phoolproof [5] is a public-key based scheme for strengthening bank transaction system. User is required to choose a bank site from the whitelist on the phone and then wait for information exchange between the phone and PC. MP-Auth [6] is a scheme that defends keylogger and phishing attacks with a cell phone by moving password input to mobile end and re-encrypting the username and password. Both Phoolproof and MP-Auth require wireless connection and wellimplemented SSL/TLS. Czeskis et al. proposed PhoneAuth [7], a smartphone-based TFA scheme to strengthen user security in authentication. Despite that PhoneAuth and CamAuth share certain similarities, there also exist substantial differences. First, PhoneAuth is built upon the origin-bound certificate, which modifies TLS to realize strong client authentication. The deployment of PhoneAuth requires modification to current TLS, web browser, and smartphone firmware, which is not practical for average users. Second, PhoneAuth relies on Bluetooth for communications between the smartphone and PC. However, Bluetooth can be subjected to a variety of attacks. The Bluetooth module of smartphone has to stay active all the time, which is certainly not power efficient for mobile devices. Recently camera-based 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. McCure et al. proposed an authentication scheme called Seeing-is-Believing (SiB) [8], which leverages the unidirectional visual channel between a 2D barcode and a camera phone for simple authentication and demonstrative identification of devices. Sexena et al. proposed a short-range device pairing protocol, VIC (Visual authentication based on Integrity Checking), which is also based on a unidirectional visual channel [9]. Another wireless communication channel (e.g., Bluetooth) has to be used to complete the pairing process. Neither SiB nor VIC is suitable for web authentication. Recently, Xie et al. proposed CamTalk, a light based communication framework for bidirectional secure information transfer between smartphones by leveraging smartphone's displaycamera channel [10].

III. SYSTEM DESIGN

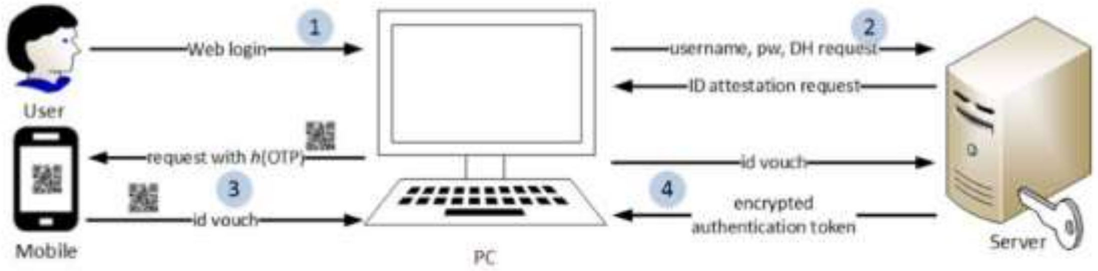

Fig1: System Architecture

CamAuth is aimed to assure the safety of net authentication through a web application in a very efficient and convenient manner. CamAuth uses a mobile device because the trustworthy second authentication issue. throughout the CamAuth authentication, the device is employed to vouch for the user's identity. Neither cellular network nor radio frequency (RF) wireless network (e.g., LAN and

Bluetooth) is employed for transferring the device's vouch, that avoids varied RF attacks. Instead, CamAuth applies actinic ray communication(ARC) through camera to acquire advantage of the safety and convenience offered by ARC. Figure 1 depicts a standard authentication method through CamAuth. the method consists of 4 interactions between concerned entities (i.e., user, PC, mobile device, and net server1). 1) A user performs an internet login through an internet browser by getting into his/her username and password either manually or mechanically through a password manager on the login webpage. 2) the online browser is activated to send the username and password (or its hash value; pw is employed to represent) beside a DiffieHellman (DH) exchange request together with its dynamically generated DH public key to the remote server. when verificatory the password, the server runs the DH algorithmic program to derive the shared secret, denoted by OTP, and sends back its identity vouch request and its DH public key. 3) The browser first computes the shared secret supported the received message so encodes the request with the hash worth of the shared secret into a barcode and renders it on the webpage. when scanning the barcode, the CamAuth app on the mobile device verifies the request and vouches for the user's identity mistreatment public key cryptography. The vouch message is encoded into another barcode, rendered on the screen, and captured by the PC's digital camera. 4) The vouch message is transferred to the server. If the validation of the vouch succeeds, the server can generate associate degree authentication token (usually a session cookie), inscribe the token with the shared secret, and send it back to the browser, that completes the authentication method.

IV. 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.