SECURE E-BANKING USING VISUAL AUTHENTICATION PROTOCOL

R.Aswin Rajesh*

T.M.Vignesh*

Mrs P.Ezhil**

ABSTRACT:

The design of secure authentication protocols is quite challenging, considering that various kinds of root kits reside in PCs (Personal Computers) to observe user's behavior and to make PCs untrusted devices. Involving human in authentication protocols, while promising, is not easy because of their limited capability of computation and memorization.Therefore, relying on users to enhance security necessarilydegrades the usability. On the other hand, relaxing assumptions and rigorous security design to improve the user experience can lead to security breaches that can harm the users' trust. we demonstrate how careful visualization design can enhance not only the security but also the usability of authentication. To that end, we propose two visual authentication protocols: one is a one-time-password protocol, and the other is a password-based authentication protocol. Through rigorous analysis, we verify that our protocols are immune to many of the challenging authentication attacks applicable in the literature.

Furthermore, using an extensive case study on a prototype of our protocols, we highlight the potential of our approach for real-world deployment: we were able to achieve a high level of usability while satisfying stringent security requirements.Index Terms—Authentication, Smartphone, Malicious code,Keylogger.

* Under Graduate Students

** Asst. Professor

Department of Information Technology, Karpaga Vinayaga College of Engineering & Technology

INTRODUCTION:

Threats against electronic and financial services can be classified into two major classes: credential stealing and channel breaking attacks. 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 bythe proper usage of a security channel such as IPSec and SSL (secure sockets layer) recent channel breaking attacks are more challenging. Indeed, "keylogging" attacks-or those that utilize session hijacking, phishing and pharming,and visual fraudulence— cannot be addressed by simplyenabling encryption.Chief among this class of attacks are keyloggers. A keylogger is a software designed to capture all of a user's keyboard strokes, and then make use of them toimpersonate a user in financial transactions.

RELATED WORKS:

Another closely related work is "Seeing-is-Believing" (SiB) which uses visual channels of 2D barcodes to resist the man-in-the-middle attack in device pairing[1]. Though we utilize similar tools by using the 2D barcodes for information representation, and the visual channel for communicating this information[1], our protocols are further more generic than those proposed in [2].Our protocols are tailored to the problem settings in hand, e-banking, with a different trust and attack model than that used in we assume that it is always trusted and immune to compromise, which means no malware can be installed on it[3]. Notice that this assumption is in line with other assumptions made on the smartphone's trust worthiness when used in similar protocols to those presented in this paper[3].Keyloggers are popular and widely reported in many contexts[4] . Slightly touched upon in this paper are keyloggers as potential attacks for credentials stealing, which are reported in and other malwares which are reported in.

Threats against electronic and financial services can be classified into two major classes: credential stealing and channel breaking attacks[5]. Of special interest are authentication protocols that use graphical passwords like those reported in and attacks on them reported in[5].

To mitigate the keylogger attack, virtual or onscreen keyboards with random keyboard arrangements are widely used in practice[6]. Both techniques, by rearranging alphabets randomly on the buttons, can frustrate simple keyloggers[6]. 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[7]. Another mitigation technique is to use the keyboard hooking prevention technique by perturbing the keyboard interrupt vector table[7].

Besides the security of an authentication protocol, both usability and deployability are equally important and critical for the acceptance of any protocol in modern computing settings. Bonneau et al[8]. have developed 25 different metrics for evaluating such aspects in an authentication scheme to compete with the existing password-based authentication that is well-accepted in practice[8]. A comparison with other works based on their usability, deplotability, and security, for othersystems and how they compare toour work, see the work in[9]. The reader is referredto for further details on the definitions those metrics, and how they apply to the various authentication mechanisms in the literature[10]. In the following, we summarize how our perform on those metrics, and thus how they compare to other protocols in the literature[11]. We limit our attention to the baseline, the password-based authentication, and a few phonebased authentication protocols[11].

EXISTING SYSTEM:

Secure authentication protocols is quite challenging, considering that various kinds of root kits reside in PCs (Personal Computers) to observe user's behavior and to make PCs untrusted devices. Involving human in authentication protocols, while promising, is not easy because of their limited capability of computation and memorization. The attacker is capable of creating a fake server to launch phishing or pharming attacks.

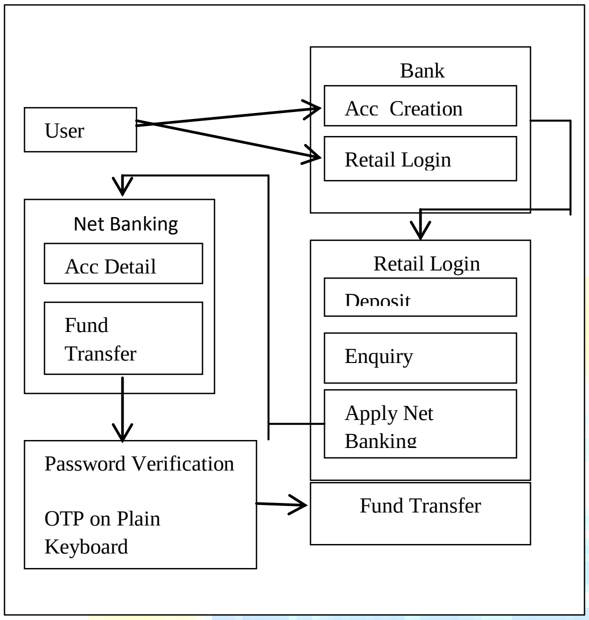
Attacks are:-

- Key Space and Brute-Force Attacker
- Keyloggers
- Malicious Software (malware)

PROPOSED SYSTEM:

The proposing two visual authentication protocols: one for password-based authentication and the other for one-time-password. Two protocols for authentication that utilizes visualization by means of augmented reality to provide both high security and high usability. We show that these protocols are secure under several real-world attacks including keyloggers. Both protocols offer advantages due to visualization both in terms of security and usability(OTP) One-Time-Password:-This protocol generates random number.Password-based authentication: uses a password shared between the Server and the user, and a randomized keyboard.

SYSTEM ARCHITECTURE:



Modules:-

Create New Account

User create a new account in our banking application to given an input for user detail in our new account registration .User detail must a valid information (ex:-phone-no, Username, etc...) after enter the user detail the form is submit to corporate. Our bank manager validate the user registration form then create an account number for an user .After the user receive an account number he/she is access the all service in our bank.

Apply Net Banking

User receives an account number he/she is entering aretail login and applies a net banking as services. This service is used to account holder view his profile and account detail then transfer the fund in another account this services are provide our bank. Banking as many services butour bank is provide net banking as a services because

fund transfer /money transfer is challengingtask for user in PCs untrusted devices. There are many attacks(ex:-keylogging, Malicious Software, etc...).

An Authentication Protocol with Password and Randomized Onscreen Keyboard

Account holder transfer the fund in another account he/she enter the account number and amount then before enter the password. Our banking application use a two visual authentication protocols (OTP)

One-Time-Password and Password-based authentication these protocols used in transfer the fund/amount in another account.

(OTP) One-Time-Password:-Each and every time therandomized OTP is generate and encrypted then form the QR code .The QR code is display the left-hand side and randomized plain keyboard is display in right-hand side account holder using his android phone scan the QR code. The QR code is decryptedusing his private key, then the OTP is appear on his mobile ,the OTP containrandomized (0 to 9) number placed in different place.

Password-based authentication:-

User views a randomized (0 to 9) number placed in different place in (4x4)matrix in his android mobile .Then the user click the password in randomized plain keyboard using the mouse with the help of OTP if the password is match the fund/amount is transfer.

CONCLUSION

We proposed and analyzed the use of userdriven visualization to improve security and user-friendliness of authentication protocols. Moreover, we have shown two realizations of protocols 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. We developed Android application of a prototype of our protocol and demonstrate its feasibility and potential in real-world deployment and operational settings for user authentication. Our work indeed opens the door for several other directions that we would like to investigate as a future work. First of all, our plan is to implement our protocol on the smart glasses such as the google glass, and conduct the user study.

REFERENCES

- [1] —. Google authenticator. http://code.google.com/p/ google-authenticator/.
- [2] —. Rsa securid. http://www.emc.com/security/rsa-securid.htm.
- [3] Cronto. http://www.cronto.com/.
- [4] —. BS ISO/IEC 18004:2006. information technology. automatic identification . and data capture techniques. ISO/IEC, 2006.
- [5] —. ZXing. http://code.google.com/p/zxing/, 2011.

- [6] D. Boneh and X. Boyen. Short signatures without random oracles. In Proc. of EUROCRYPT, pages 56–73, 2004.
- [7] 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. In Security and Privacy (SP), 2012 IEEE Symposium on, pages 553–567. IEEE, 2012.
- [8] J. Brown. Zbar bar code reader, zbar android sdk 0.2. http://zbar. sourceforge.net/, April 2012.
- [9] C.-H. O. Chen, C.-W. Chen, C. Kuo, Y.-H. Lai, J. M. McCune, A. Studer, A. Perrig, B.-Y. Yang, and T.-C. Wu. Gangs: gather, authenticate 'n group securely. In J. J. Garcia-Luna-Aceves, R. Sivakumar, and P. Steenkiste, editors, MOBICOM, pages 92–103. ACM, 2008.
- [10] S. Chiasson, P. van Oorschot, and R. Biddle. Graphical password authentication using cued click points. In Proc. of ESORICS, 2008.
- [11] D. Crockford. The application/json media type for javascript object notation (json). http://www.ietf.org/rfc/rfc4627.txt?number=4627, July 2006.