© 2015 IJSRSET | Volume 1 | Issue 1 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

# Secure Internet Banking with Visual Authentication Protocol

**Saraswathi. R, Shanmathi. G, Preethi. P, Arul. U**
Dhanalakshmi College of Engineering, Kancheepuram District, Tamilnadu, India

## ABSTRACT

Keylogging or keyboard capturing, is the action of recording (or logging) the keys struck on a keyboard typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. It also has very legitimate uses in studies of human-computer interaction. There are numerous keylogging methods ranging from hardware and software-based approaches Involving human in authentication protocols, while promising, is not easy because of their limited capability of computation and memorization. We demonstrate how careful visualization design can enhance not only the security but also the usability of authentication. We propose two visual authentication protocols: one is a one-time-password protocol, and the other is a password-based authentication protocol. Our approach for real-world deployment: we were able to achieve a high level of usability while satisfying stringent security requirements.

**Keywords:** Authentication,QR code,Android mobile, keylogger.

## I. INTRODUCTION

Threats against financial services in bank can be classified into two major classes credential stealing and channel breaking attacks[1]. Attacks such as users, identifiers, passwords and keys can be stolen by an attacker when they are not managed properly. Channel breaking attacks, which allow another form of exploitation[8]. The proper usage of a security channel such as IPSec and SSL (secure socket layer), recent channel breaking attacks are more challenging [5]. Indeed, "keylogging" attacks are those that utilize session hijacking, phishing and Pharming and visual fraudulence cannot be addressed by simply enabling encryption. To mitigate the keylogger attack[2], virtual or onscreen keyboards with random keyboard arrangements are widely used in practice. Both techniques, by rearranging alphabets randomly on the buttons, can frustrate simple keyloggers. 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.

**Existing system :** 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[6]. 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[4].

## II. METHODS AND MATERIAL

**Proposed System:** The existing system has various drawbacks such as Key Space and Brute-Force Attacker, Keyloggers, Malicious Software (malware), Shoulder-Surfing Attacks to avoid that we are 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. One-Time-Password: This protocol generates random number for authentication.

Password-based authentication: uses a password shared between the Server and the user, and a randomized keyboard.

**Proposed algorithm for implementation:** The algorithm used to implement our project is RSA algorithm. The steps of the RSA algorithm is as follows

**Step: 1.** Choose two very large random prime integers: p and q

**Step: 2.** Compute n and φ(n):

$n = pq$ and $\varphi(n) = (p-1)(q-1)$

**Step: 3.** Choose an integer e, $1 < e < \varphi(n)$ such that:

$\gcd(e, \varphi(n)) = 1$(where gcd means greatest common denominator)

**Step: 4**. Compute d, $1 < d < \varphi(n)$ such that:

$ed \equiv 1 \pmod{\varphi(n)}$

public key is (n, e) and private key is (n, d).

**Encryption**-The cipher text C is found by the equation '$C = M^e \bmod n$' where M is the original message.

**Decryption**-The message M can be found form the cipher text C by the equation '$M = C^d \bmod n$'.

## Types of attacks

We assume that the channel between the server and the user's terminal is secured with an SSL[5] connection,which is in fact a very realistic assumption in most electronic banking systems. Second, we assume that the server is secured by every means and is immune to every attack by the attacker hence the attacker's concern is not breaking into the server but attacking the user. Finally, with respect to the keylogger attack, we assume that the keylogger always resides on the terminal. As for the attacker model, we assume a malicious attacker with high incentives of breaking the security of the system. The attacker is capable of doing any of the following: The attacker has a full control over the terminal. While residing in a user's terminal, the attacker can capture user's credentials such as a password, a private key, and OTP (one time password) token string. The attacker can deceive a user by showing a genuine-looking page that actually transfers money to the attacker's account with the captured credentials that she obtained from the compromised terminal. Or just after a user successfully gets authenticated with a valid credential, the attacker can hijack the authenticated session. The attacker is capable of creating a fake server to launch.

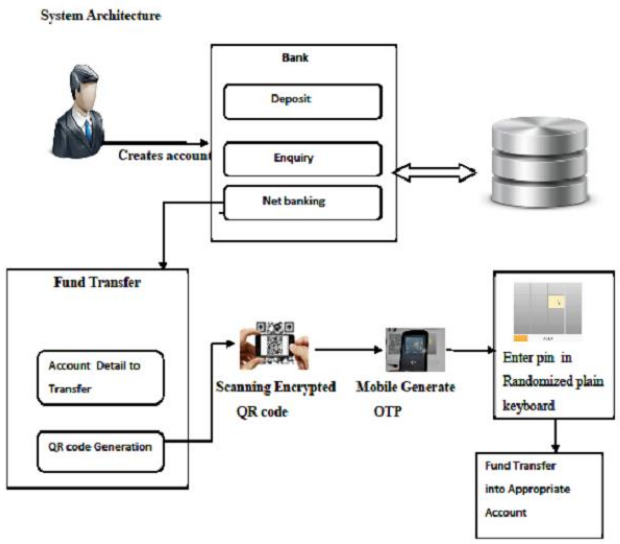


Figure 1: System Architecture

## III. RESULTS AND DISCUSSION

### A. Account Generation

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.

### B. Retail login

User receives an account number he/she is entering a retail 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.

### C. Apply Net Banking

Account holder transfers the fund in another account he/she enter the password. For password verification, we use two visual authentication protocols One-Time-Password and Password-based authentication. Banking as many services but our bank is provide net banking as a services because fund transfer /money transfer is

challenging task for user in PCs untrusted devices. There are many attacks (ex:-key logging, Malicious Software, etc...).

### D. QRcode generation

The QR code is displayed in an encrypted form on the left-hand side and randomized plain keyboard is display on the right-hand side of the system. The QR code is decrypted by scanning in android phone. then the OTP is appear on his mobile ,the OTP contain randomized (0 to 9) number placed in different place, then the user click the password in randomized plain keyboard using the mouse with the help of OTP.

### E. Performance Analysis

The existing system has various drawbacks such as Key Space and Brute-Force Attacker, Keyloggers, Malicious Software (malware), Shoulder-Surfing Attacks to avoid that we are proposing two visual authentication protocols: one for password-based authentication, and the other for one-time-password. Another enhancement is IMEI security. Main purpose of this is, to avoid malicious transaction.

## IV. CONCLUSION

In this paper, we proposed and analyzed the use of user driven 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. In this project we developed enhancement is offline transaction. Mostly transactions are done through online only. But for time consuming and quick transaction we proposed offline transaction. In offline transaction user generate one file, inside that file user account-no, transaction amount, and etc. are available. Those details are prepared by user when they are in offline. When user entered into online, they just load this file into the applications for fund transaction. Using this offline transaction, user timings are more consumed. Another enhancement is IMEI security. Main purpose of this is, to avoid malicious transaction. When other user knows my username and password means, they can use my details for fund transfer without my knowledge. To avoid this we are providing IMEI security. Every user registration server stores their IMEI number into their database. Another malicious user, use my username and password in their mobiles means IMEI no vary so proper transaction will not occur.

## V. REFERENCES


[1] A. Hiltgen, T. Kramp, and T. Weigold. Secure internet bankingauthentication. IEEE Security and Privacy, 4:21–29, March 2006.

[2] A. Slowinska and H. Bos. Pointless tainting?: evaluating the practicalityof pointer tainting. In Proc. of ACM EuroSys, pages 61–74, 2009.

[3] B. Parno, C. Kuo, and A. Perrig. Phoolproof phishing prevention. InProc. of Financial Cryptography, pages 1–19, 2006.

[4] E. Hayashi, R. Dhamija, N. Christin, and A. Perrig. Use your illusion: secure authentication usable anywhere. In Proc. of ACM SOUPS, 2008.

[5] E. Rescorla. SSL and TLS: designing and building secure systems. Addison-Wesley, 2001.

[6] H. Yin, D. Song, M. Egele, C. Kruegel, and E. Kirda. Panorama: capturing system-wide information flow for malware detection

[7] J. M. McCune, A. Perrig, and M. K. Reiter. Seeing-is-believing: Using camera phones for human-verifiable authentication. In Proc. of IEEE Symposium on Security and Privacy, pages 110–124, 2005.

[8] N. Hopper and M. Blum. Secure human identification protocols. In Proc. of ASIACRYPT, 2001. Communications of the ACM, 24(11):770–772, 1981.