ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 10, October 2016

Secure Internet Banking Using QR Code Based Visual Authentication

[1] Mrs. Kashmira M. Ambavane [2] Mrs.Amruta D. Harpude [3] Prof Sonali Tidke [4] Prof Roshani Dange
SRTTC-VIT Kamshet Campus

Abstract:- **In this paper, we proposed and analyzed the use of user driven visualization to improve security and user-friendliness of authentication protocols. The project aims at creation of a Secure Internet Banking System. This will be accessible to all users who have a valid user_id and password for this Smartphone App. This project gives an opportunity to the customer to have a secure online transaction without moving to the bank. We give the security in two terms, firstly QR code based security and secondly the Virtual keyboard for password. Morever, we have shown two realization of protocols that not only improve the user experience but also resist challenging attacks, such as the key logger and malware attacks. Our protocols utilize simple technologies available in most of the box smart phone 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.**

Key Words: **Authentication, OTP, QR code, Smartphone..**

I. INTRODUCTION

Nowadays, Smartphone's have become the essential tool in day-to-day life, through which human beings are connected to the cyberspace. Smartphone's or tabs are not only used for providing a user with use full or interesting information perhaps it also provides sensitive services like Mobile Internet Banking and corporate services. To identify the user, user authentication is required to prevent the user from unauthorized access[1].Although many Authentication mechanisms are available yet passwords are not that secure and it may led to financial loss or corporate data disclosure. Whenever Smartphone's are used for Security purpose it is not that secure because they are widely used in public places.
Hence passwords are prime target of attackers, for economically-motivated exploits including those targeting online bank accounts and identity theft.
Since password is hacked during authentication when the user inputs his password, we focus on improving the password security for the users.

In fact, the main class of attacks is Key loggers. Key loggers are often referred as Spyware that has the capability to record every keys stroke. Some Key loggers programs will also record any email addresses you use and website URLS. Unfortunately key loggers can also be embedded in Spyware allowing your information to be transmitted to any unknown third party.

To mitigate the key logger attack, 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 key loggers. Unfortunately, the key logger, 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[2].

However, our goal is to provide security in terms of QR code and Password Hacking.

II. LITERATURE REVIEW

1) Key loggers

A key logger is also called as keystroke logger. A key logger is nothing but small program or a hardware device that monitors each keystroke that a user types on a keyboard. When the user types, each keystroke is saved in its own hard drive. Physical access to the users computer is not required by the key logger program. Protocol 1. Authentication in this protocol is based on a random string generated by the server. Private key of the user is verified against the public key of the user by the random key encryption. The main purpose of OTP is that it is of one time use. As it is used only once the key logger or the attacker will obviously not be able to know the OTP because as that OTP will not be reused again for future authentication.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 10, October 2016

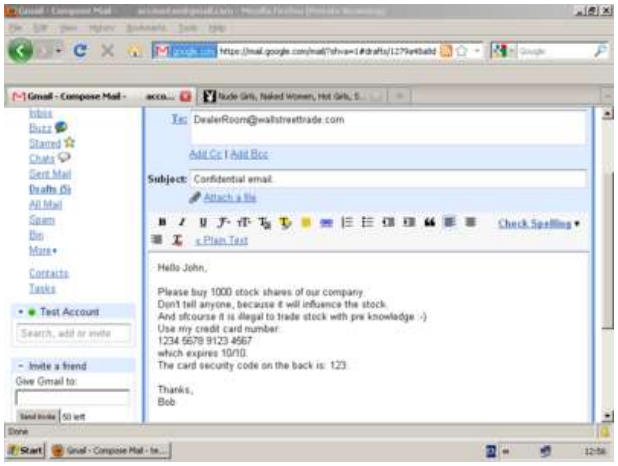

Fig 1:Key Logger Attack[4]

2) Shoulder-surfing attacks

Shoulder surfing is nothing but the direct observation technique such as looking over someone's shoulder to get the information. We can easily get the information of another person in crowded place using shoulder surfing. Not only by standing close to person shouldering attack can be done but also shoulder surfing can be done at a long distance by using binoculars.

Our used protocols make use of Virtual keyboard which avoids the Shouldering Attack.[5]

Fig 2: Shoulder Surfing Attack [6]

III. EXISTING SYSTEM

1) Authentication with Random Strings

We used an authentication protocol named One time password (OTP).The Protocol works as follows:

1. The ID is send to the user when the user connects to the Server.
2. The server retrieves the user's public key from the database by using the users ID. A fresh random string OTP is then picked by the server and encrypts it with the public key.
3. In the terminal, a QR code is displayed prompting the user to type in the string.
4. The QR code is decoded by the user. Because the random string is encrypted with users public key, the user can read the OTP string only through her Smartphone and type in the OTP in the terminal with a physical keyboard.

5. The server checks the result and if it matches what the server has sent earlier, the user is authenticated. Otherwise, the user is denied. In this protocol, OTP is any combination of numbers whose length is depending on the security level required.[2]

2) An Authentication Protocol with Password and Randomized Onscreen Keyboard

Our second protocol uses a password shared between the server and the user, and a randomized keyboard. The protocol works as follows:

1. The ID is send to the user when the user connects to the Server.
2. To retrieve the users public key from the database the server checks the ID. The server prepares a random permutation of a keyboard arrangement, and encrypts it with the public key. The server sends the result with a blank keyboard.
3. In the user's terminal, a QR code is displayed together with a blank keyboard. Because the onscreen keyboard does not have any alphabet on it, the user cannot input her password. Now, the user executes her smart phone application which first decodes the QR code to get the cipher text. The cipher text is then decrypted by the smart phone application with the private key of the user to display the result on the Smartphone's screen.

4. The server checks whether the password is correct or not
5. If the password is wrong then again the new virtual keyboard is sent on his mail.[2]

IV. PROPOSED SYSTEM

1) SCOPE

In this paper, we implemented two Visual Authentication protocols, one for Password based authentication and another for one-time password (OTP).By proposing these two authentication protocols we demonstrate how visualization can enhance not only security but also usability. Based on the study of these two protocols we height light the potential of our protocols in

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 10, October 2016

Real-world deployment. These two protocols are secure under not only by several real world attacks but also by the key loggers. We have implemented the use of these protocols in the form of Android Application.

2) ARCHITECTURE

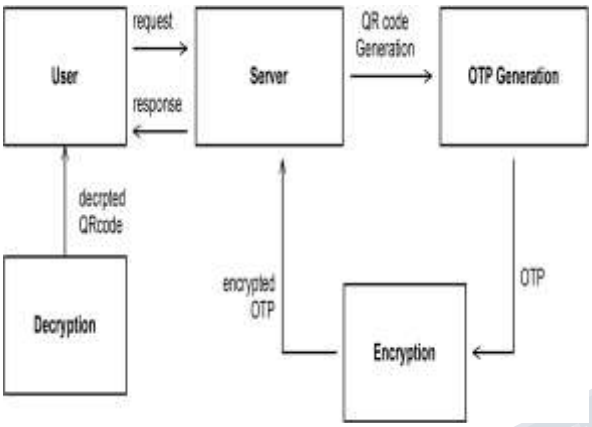

Fig 3: Architecture

In the above architecture, when the user creates an account in the Application, the details are stored in the server. After creating the account a QR code is generated. For each user a unique OTP is generated. During each transaction a unique OTP is generated which is send to the server in encrypted form. And then the server sends that OTP to the user as a response to the users request.

In the above figure the concept of decryption is that the QR code generated by this App can be scanned and decrypted if it is scanned by the scanner of this App only.

3) QR code Generation

QR code is a type of matrix barcode consisting of an array of black and white squares. These black and white squares are used to store information in encrypted form. A QR code is a two dimensional barcode. Application of QR code are product tracking, item idenfication, document management and general marketing.

QR code is better than barcode because barcode can store information in horizontal direction whereas QR code can hold in vertical and horizontal both directions. QR code carry information in smaller space compared to barcode.[3]

Fig 6: QR code

Fig 7:Barcode

Our first approach is to provide security to QR code. Nowadays many banking apps are available for online transaction. Basically the QR code can be scanned by any other scanner and our information gets decrypted easily. But the Application developed by us allows the QR code to be scanned by the scanner of only our Application.

Our second approach is to provide security for password. Password hacking is nowadays a common problem. Password is hacked by the key loggers. Due to this our account can be hacked easily. So we are implementing the concept of virtual keyboard which reduces the chances of password hacking. When a user creates an account in this application a virtual keyboard will be sent on his mail. This keyboard will be unique for each user. For example, if your password is 693,but when entering in the normal keyboard you need to press 123,then internally your password will be entered as 693.This protects you from Shouldering Attack.

Fig 4: Virtual Keyboard

Fig 5: Normal Keyboard

V. CONCLUSION

In this paper, we proposed the two Authentication protocols for Secure Internet Banking, which provides a secure and user-friendly approach for Secure online transaction.. Moreover, we developed Android application of a prototype of our protocol and demonstrate its feasibility and potential in real-world deployment. It also prevents the user from different attacks such as key logger attack and shoulder surfing attack. Finally, reporting on user studies that will benefit from a wide deployment and acceptance of our protocols would be a parallel future work to consider as well.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 10, October 2016

REFRENCES

[1] Q. Yan, J. Han, Y. Li, J. Zhou, and R.H. Deng, "Designing Leakage Resilient Password Entry on Touchscreen Mobile Devices"

[2] Keylogging-Resistant Visual Authentication Protocols, DaeHun Nyang, Member, IEEE, Aziz Mohaisen, Member, IEEE, and Jeonil Kang, Member, IEEE

[3] https://en.wikipedia.org/wiki/QR_code

[4] https://en.wikipedia.org/wiki/Keystroke_loggingssss

[5]https://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security)

[6] http://www.itlawtoday.com/2013/08/nj-13th-state-to-protect-employees-social-media-logins-passwords/