Secure Authentication Using PTP

M. Gokula Krishnan[1], R. Harish Chandar[1] and K. Esther Rani[2]
1-Student and 2-Assistant Professor, Department of IT,
Parisutham Institute of Technology and Science, Thanjavur, Tamilnadu

***Abstract*— Generally there are various kinds of attacks reside in PCs (Personal Computers),which makes our system a un trusted device. The humans cannot have the ability of computing or memorizing an authentication protocols. Any how we need to be in a secure and reliable part to make our information a private one. We demonstrate how careful visualization design can enhance not only the security but also the usability of authentication. Finally we propose password through phone (PTP) algorithm. This makes our project more secure and authenticated comparing to the existing one.**

Keywords: Secure,Authentication,PTP.

I. INTRODUCTION

INTERNET is a global system consists of interconnected computer networks it uses Standard Internet protocol. Nowadays in financial services there are so many hurdles. This type of attack is a credential stealing. At present each and everyone is aware of using PC's. There are so many advantages in usage of personal computers and one more face is there for personal computer is disadvantages. Improper maintenance of PC's will get affected by malicious software .It is used by the attackers to steal the user's credential which comprises of user's name, passwords and identifiers. Sometimes this problems can be rectified when they have highly secured system.

Attacks can be reduced by simply using the encryption technique but it is not quite capable for all the attacks. Among those attacks the major attack is the presence of keylogger. Keylogger is often called as keystroke logging or keyboard capturing. Keylogger is the surveillance software

Which is used to record the user's data which is entered through the keyboard. So the persons using the keyboard is unaware that there actions are being monitored.

Keylogger which control over the computer and can capture every event. Shoulder Surfing attack is also seems to be similar to the keylogger attack. Many graphical passwords technique have been used to reduce the shoulder surfing attack.

Our method to solving this problem is to introduce an device which connects the user and a terminal. This device will acts act's a intermediate and then the each interaction between the user and the device is been visualized through a Quick Response (QR) code. Quick Response have fast readability and higher storage capacity. Required data's were extracted from the pattern of QR code. Keyloggers presence is pervasive it can be present in public internet café and even in personal computers. This attack makes even worse when the user processing transactions via online at that moment he/she will provide their bank details. For example the PIN number, account password. So, the user unaware about the keyboard capturing. Any how we need to be in a secure so we need the visual authentication and it is done by through the Smartphone. Finally we propose the Password through Phone algorithm. In this paper we demonstrate the usage of visual authentication and also its security level.

By using visual authentication the security level is upto the mark and the attackers can't easily breach the security. Here we are using the smartphones with the camera attachments.

QR code will act's as connecter between the user and the terminal. Smartphone contains numerous applications for all type of sectors.

The usage of Smartphone is getting hike by each and every day and there is no destination for the technologies. QR code scanner application is been used to scan the code and to extract the information and then details which are resides in code.

This quick response code which is present in websites to reduce the information capacity. For example, suppose in the website the user wants to go another page and the link is been present in QR code to reduce the contents in page. Here the user needs to scan the quick response code and it's done by using the QR code scanner application.

Fig 1Android application

II. MODELLING AND REFERENCE

In this paper we demonstrate the usage of visual authentication and also its security level. For the visual authentication there are some protocols like one time password and password based authentication protocol. These protocols are very much in the usage for the websites which contains the user's confidential details and these details mostly get's attacked when the system is in unsecure state and if the system is in a lower security level then it is easy for the attackers to steal the user's confidential details like password, PIN number.

A. *Keylogger Attack:*

Keylogger is a software program that monitors each and every keystroke a user types on a specific computer keyboard. This type of attacks were present in browsing centers and also in the personal computers. Sometimes the keylogger or system monitors is a hardware device and it is used to observes the user's behavior and the device is small like battery sized plug which is been acts as a connector between the computer and user's keyboard.

As the user types the details then the each keystroke is been saved in the keyboard logger. Finally the person who installed the keyboard logger in the computer must return and to physically remove the device in case to access the information's which are present in the device. Following graph shows the keylogger and its effect.

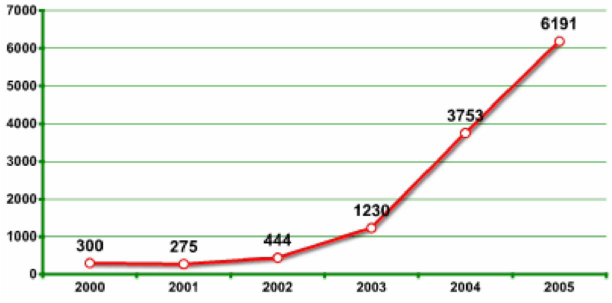


Fig 2 Keylogger Graph

B. QR Code:

QR Code is defined as a Quick Response code and it is a type of matrix barcode. It is a machine readable optical label which comprises of information about the item which it is attached. QR code is also known as a 2D barcode and it contains the black square dots which are arranged in a square grid on a white background. Information's can be added in both horizontal and vertical components of image.

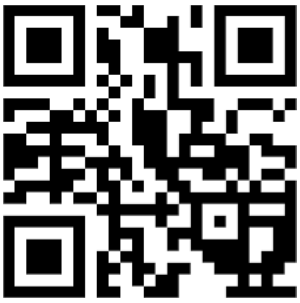


Fig 3QR Code

Quick Response code scanner is a mobile application which is used to scan the QR code. To use QR codes conveniently you must have a smartphone equipped with a camera and a QR code reader/scanner application feature. To download the mobile application for the smartphone visit your phone's app store (Examples Play store, Apple App store, BlackBerry App World).

So, now that you have the tools which are required and next let's move on to the scanning. Initially find yourself a code. Then open the application which you have downloaded to scan the code.

Steady your hand while the QR code is centered on the screen. As soon as it is done scanning the information it contains example such as videos, webpage URL's etc were stored in QR code.

Fig 4 QR Code Scanning

Fig 5 Scanning on process from top to bottom

III. RELATED WORKS

There are much more problems generally in the authentication. Some of the reference papers which deals with the e-banking and then the online transactions. Even some papers related to the secure authentication by using graphical passwords.

S.Chiasson, P.vanOorschot and R.Biddle [1] which is the paper directly deals with the secure authentication by using graphical passwords instead of using as a normal passwords. Technology used in this paper is cued click points (CCP).Authentication is specially discussed in [2], [5],[6],[7]and they are used especially in e-banking.In the banking sectors the visual authentication protocols have been used and it is been discussed in [9], [10].

The visual authentication protocol used here is a onetime password. Attacks for the visual authentication is been briefly explained in the papers [4],[8].

Similar related work is seeing is believing which uses the barcodes to control the man-in-middle attack in discussed in [12].

In the open network there is a drawback in which the workstation cannot be trusted to identify the users. For this problem the Kerberos provides a solution by providing the trusted third party approach which is discussed in [13].

IV. EXISTING SYSTEM

In the existing system whenever the user types a password in a bank's sign in box or any other account. Those details were very much confidential. At that time the user enters the details like password, PIN number to access the account the keylogger will intercept the password.

Keylogger is a monitoring software and it is used to observe the user's behavior. Keylogger or system monitors is a hardware device and it is used to observes the user's behavior and the device is small like battery sized plug which is been acts as a connector between the computer and user's keyboard. Suppose if the user wants to perform financial transactions by using browsing center is always the biggest concern because is that a user's password is likely to be stolen from those computers.

Key loggers are often root kited which are hard to detect since they will not display in task manager process list.

User's confidential details are get easily tracked and it is been recorded in the keylogger.

In the existing system the for authentication the password is been provided by the user to access the account and to login.

Here also for the visual authentication the QR (Quick Response) code is used. Initially QR code scanner should be downloaded from the mobile application store.

Quick response contains the information which has been stored in the code. Information's can be added in both horizontal and vertical components of image.

After scanning the quick response code then the keyboard will show up in screen and then the password is been entered through the computer.

V. PROBLEM STATEMENT

Major problem is presence of the keylogger and it breaches the ordinary security. Keylogger is a software program that monitors each and every keystroke a user types on a specific computer keyboard. This type of attacks was present in browsing centers and also in the personal computers.

Sometimes the keylogger or system monitors is a hardware device and it is used to observes the user's behavior and the device is small like battery sized plug which is been acts as a connector between the computer and user's keyboard.

As the user types the details then the each keystroke is been saved in the keyboard logger.

Finally the person who installed the keyboard logger in the computer must return and to physically remove the device in case to access the information's which are present in the device.

VI. PROPOSED SYSTEM

Our approach is to solve the problems which are in the existing system. Problem is solved by through introducing the intermediate device that will connects the user and terminal.

We propose Password through Phone (PTP) algorithm by this method the interception of keylogger will be avoided and then there is no usage of computer.

This approach can be used in the ATM centers as well because while the user inserts the debit card and then they will enter the PIN number. It can be easily stolen by the third person who needs our credential details. To avoid this type attacks the PTP is used by the way of scanning QR code from the screen and then the user can type the PIN number via phone. This will be more secure than by using keyboard. So, for the online transactions is been quite safe and it is having visual authentication. In this way the password through phone technique will be used to keep the confidential details in a secure manner.

VII. WORKING AND RELATED TECHNIQUES

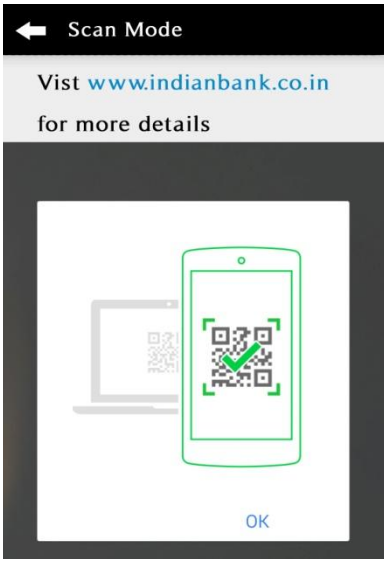
In this initially for to connect the user and the terminal the quick response code is used and it contains the information and it can't able to see. Information present in code can be seen only after the code get's scanned. Initially for this the mobile application is required that is QR code scanner.

Then user wants to enter the bank other some other details and if the details are confidential then it requires more security. For that the visual authentication is more important and the page which it has quick response code.

User needs to scan the entire QR code by using the mobile application. And the code get's started to scan from the top to the bottom.

After the user finished scanning process then the user's needs to provide the most confidential PIN number or any passwords. The following example shows to check the account balance.

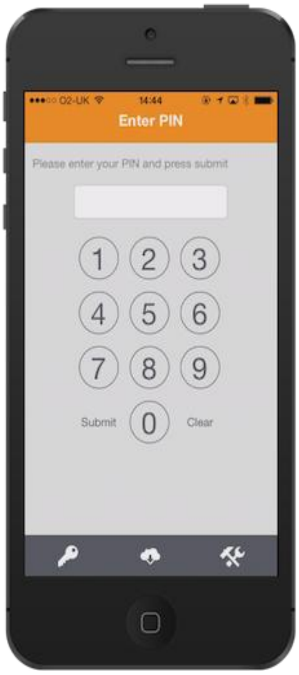
Fig 6 QR code



Scan Mode

Vist www.indianbank.co.in for more details

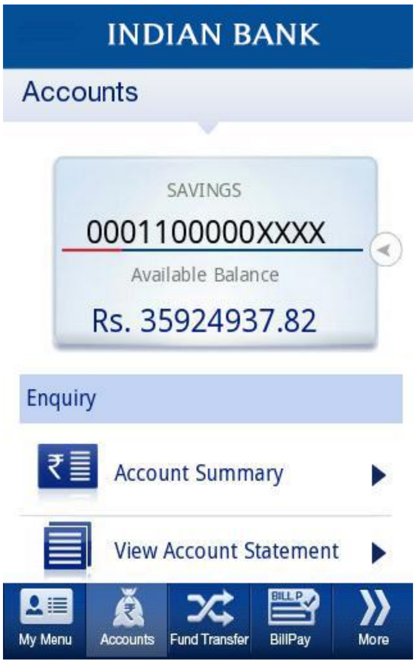
Fig 7 QR code scanned successfully



Enter PIN

Please enter your PIN and press submit

Fig 8PIN number



INDIAN BANK

Accounts

SAVINGS

0001100000XXXX

Available Balance

Rs. 35924937.82

Enquiry

Fig 9 Account Balance

In order to do the online transactions and also to check the account balance of the user and it is been easily verified by using the mobile phone through by the QR code scanner and then by providing password through mobile.

PTP technique is been used to provide the confidential details of the user through by the mobile phone. This technique provides more security and also it establish the visual authentication.

Even the PTP technique is been used in the all the fields where the user needs to provide the confidential details. By this technique the details were kept in a secure manner.

VIII. APPLICATIONS

There are some applications that are essential in day to day life and the applications were most essential for the humans.

Applications in which it requires the authentication and it needs to be in secure manner. Applications are,

In the Banking sector for to do online transactions and to check the account balance and the QR code is used to scan and then the password and also the PIN number is been provided.

Even though the user can easily get the money from the ATM centers easily but nowadays there are some attacks to steal the user details such as PIN number, OTP, Passwords. OTP is a short time password and it is defined as a One Time Password. A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password based authentication.

IX. CONCLUSION

In this paper we analyze the user's problem while giving the credential details through by the keyboard of the computers.

This type of stealing is called credential stealing. This problem makes people even more worse.

We proposed the password through phone technique by which the security level gets increased better. The design we propose is a simple by using mobile phones and it is capable to acts as terminal.

Second, we are using quick response code that is the code which is acts as a connector or a bridge between the user and the terminal. It is a machine readable optical label which comprises of information about the item which it is attached. QR code is also known as a 2D barcode.

From this paper the secure login of the user can be implemented. And then the usability, deployability and security can be achieved.

There are some many threats and attacks are possible in all fields especially in the banking sector there are more attacks were possible. To overcome some of those attacks we propose the PTP (Password Through Phone) technique.PTP technique is been used to provide the confidential details of the user through by the mobile phone. This technique provide more security and also it establish the visual authentication.

Finally the proposed will increases the security level and so the attacks can be reduced by this method. By this technique the user experience and then security is been improved. By controlling the attacks the performance get's improved.

X. REFERENCES

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

[2] S. Chiasson, P. van Oorschot, and R. Biddle. Graphical password authentication using cued click points. In Proc. of ESORICS, 2008.

[3] L. Lamport. Password authentication with insecure communication.Communications of the ACM, 24(11):770–772, 1981.

[4] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd. Reducing shoulder- surfing by using gaze-based password entry. In Proc. of ACM SOUPS, pages 13–19, 2007.

[5] X. Suo, Y. Zhu, and G. Owen. Graphical passwords: A survey. IEEE Computer, 2005.

[6] D. Boneh and X. Boyen. Short signatures without random oracles. InProc. of EUROCRYPT, pages 56–73, 2004

[7] J. Thorpe and P. van Oorschot. Human-seeded attacks and exploiting hot-spots in graphical passwords. In Proc. of USENIX Security, 2007.

[8] T. Holz, M. Engelberth, and F. Freiling. Learning more about the underground economy: a case-study of keyloggers and dropzones. In Proc. of ESORICS, pages 1–18, 2009.

[9] M. Naor and B. Pinkas. Visual authentication and identification. In Proc. of CRYPTO, 1997.

[10] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA:Using hard AI problems for security," in *Proc. Eurocrypt*, 2003, pp. 294–311.

[11] D. MRaihi, S. Machani, M. Pei, and J. Rydell. Totp: Time-based one-time password algorithm. Internet Request for Comments – RFC 6238, 2010.

[12] J. M. McCune, A. Perrig, and M. K. Reiter. Seeing-is-believing: using camera phones for human-verifiable authentication. International Journal of Security and Networks, 4(1/2):43–56, 2009.

[13] J. Steiner, C. Neuman, and J. Schiller. Kerberos: An authentication service for open networks. In Proc. of USENIX Annual Tech Conference, pages 191–201, 1988.

[14] H. Krawczyk, M. Bellare, and R. Canetti. Hmac: Keyed-hashing formessage authentication. RFC, 1997.

[15] J.Lim.Defeat spyware with anti-screen capture technology using visual persistence. In proc.of ACM SOUPS, pages 147-148,2007.