International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

Enhancement in Card Payment system

Chetan Bagade[1], Ketan Bagade[2], Akshay Deshmukh[3], Tejas Rede[4], Prof. R.M.Kedar[5]

[1,2,3,4] Students, Computer Dept. K.J.Collage of Engineering Management And Research
[5]Profesosr of K.J.collage of Engineering management And Research

---

Abstract - *As per the recent RBI Mandate, all customers who have used their credit card at an international Point Of Sale (POS) terminal will have to be re-carded with a Chip+PIN credit card. A chip is a small microchip embedded in your credit card. It is encrypted, so that transactions are more secure with that card. The Chip+PIN card is a superior level of security on your card, inline with best global practices of security of transactions When you use a Chip+PIN credit card at a POS terminal, the POS machine will prompt you for your PIN to be entered, you are required to enter the Credit Card ATM PIN in the terminal and complete the transaction. To complete the transaction, we need to provide 4 digit PIN number into that device. the biggest threat lies with susceptibility of the pin entry process to direct observational attack, such as human shouldering and camera based recording. We suspect a security thread in this process while providing PIN in front of friends, relative or unknown person, it is attack by Shoulder attack. Main aim of this system is to help users in performing their transactions in more secure way also we provides a security for digital transaction by implementing card payment system along with permission of authorized device. This help to prevent shoulder surng attack with the concept of concealing the password object information which is applicable for all Electronic payment system. We provide security by forcing user to enter his password directly by performing certain mental task to drive indirect correct password.*

***Key Words*: Security, Authentication, AESSHA 256, POS security, ATM security**

1. INTRODUCTION

Whenever shopper swap user debit card for payment, bank server notify user on his mobile to enter PIN number. User can now enter PIN using his/her mobile. Even user is free to provide number as YES/NO or any pattern which he can change on daily or monthly basis.

We found a problem when user is typing his/her PIN number in front of merchant or relatives or any other person. This is a type of Shoulder Attack. To avoid this problem we developed a system that provide enhancement in security issue.

The entry of a password can easily be observed by nearby adversaries in crowded places, aided by vision enhancing and/or recording devices, and the information that should be kept secret is leaked in a relatively non-technical manner. Even partial information leakage can be greatly harmful, since users tend to use similar or even identical passwords on multiple systems, some of which may be more important than others. The whole secret PIN could be leaked through even a single authentication session. Since PINs are so popularly used in a variety of common devices, such as smart phones, automated teller machines (ATM), and point of-sale (PoS) terminals, there is a great need for a secure PIN entry scheme that does not remarkable sacrifice usability. Various security enforcement methods have been proposed to deal with this situation, but achieving both security and usability still remains a challenging goal.

CURRENT SCENARIO:

Step 1: The merchant inserts your card at a PIN enabled POS machine..

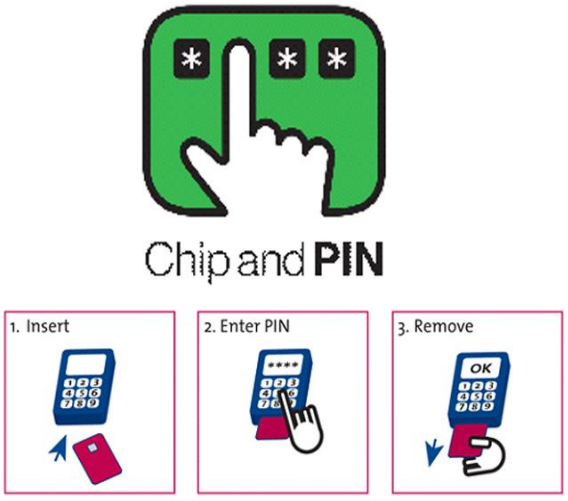
Step 2: He enters the transaction amount.

Step 3: The machine trigger for a PIN to be entered by you.

Step 4: You enter your Credit Card ATM PIN in the machine.

Step 5: On entering the correct PIN the transaction is confirmed and completed.

Step 6: For VDU(Visual Display Unit)without PIN authentication support, your new Chip+PIN credit card shall continue to support the regular signature mode.



2. LITERATURE SURVEY

1. A PIN Entry Method Strong Against Shoulder Surfing

Personal identification numbers (PINs) are obtained by shoulder surfing, through the use of mirrors or concealed small cameras. Both elements, the PIN and the card, are generally enough to give the criminal full access to the victim's account. In this paper, we present different PIN entry methods to which we refer as cognitive trapdoor games. These methods make it significantly harder for a criminal to obtain PINs even if he fully observes the entire input and output of a PIN entry procedure. We also present the plan of probabilistic cognitive trapdoor games, which offer flexibility to shoulder surfing even if the criminal records a PIN entry procedure with a camera. We studied the security as well as the usability of our methods, the results of which we also present in the paper.

2. Preventing Shoulder-Surfing Attack with the Concept of Concealing the Password Objects' Information

Traditionally, picture-based password systems employ password objects (pictures/icons/symbols) as input during an authentication session, thus making them vulnerable to "shoulder-surfing" attack because the visual interface by function is easily observed by others. Recent software-based approaches attempt to minimize this threat by requiring users to enter their passwords indirectly by performing certain mental tasks to derive the indirect password, thus concealing the user's actual password. However, weaknesses in the positioning of divert and password objects introduce usability and security issues. In this paper, a new method, which conceals information about the password objects as much as possible, is proposed. Besides concealing the password objects and the number of password objects, the proposed method allows both password and diverter objects to be used as the challenge set's input. The correctly entered password appears to be random and can only be derived with the knowledge of the full set of password objects. Therefore, it would be hard for a shoulder-surfing adversary to identify the user's real password. Simulation results indicate that the correct input object and its location are random for each challenge set, thus preventing frequency of occurrence analysis attack. User study outcome show that the proposed method is able to prevent shoulder-surfing attack.

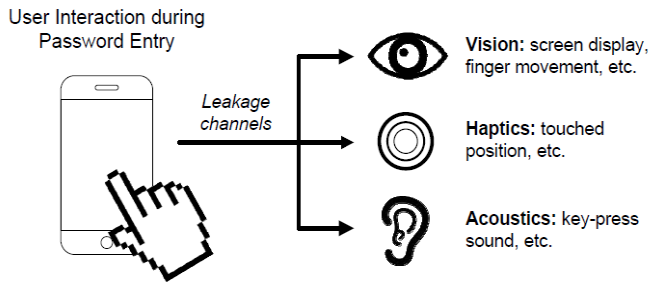


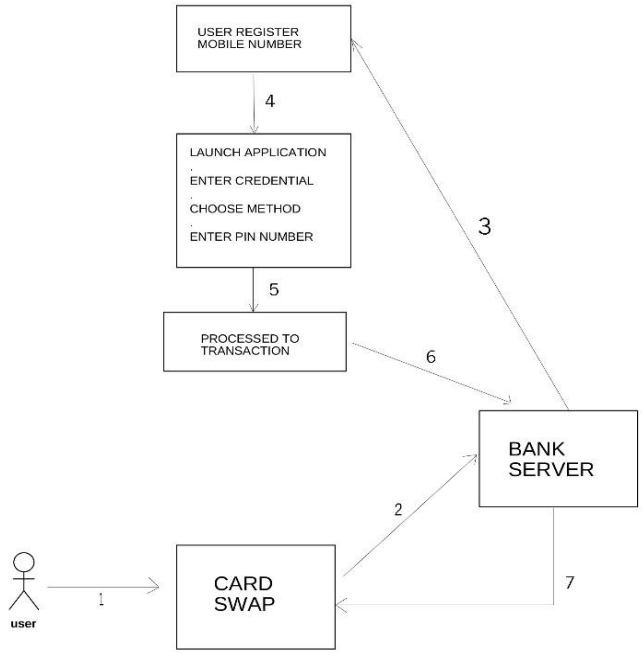
Figure 1: Attack scenarios

3. PROPOSED SYSTEM

In our system first user ask for payment, After user insert card in POS machine. Now user enter amount on POS machine after that POS machine send acknowledgement to bank server.

After sending acknowledgement to bank server, bank server checks the detail and launch application on that user mobile phone which have android operating system. User have enter the credential on login page. After that user have to select method for entering PIN for payment. The method selected by user will be use for another future transaction.

Now user can enter his/her pin according to selected method. Now user can finish transaction and bank server will send success acknowledgement to POS machine and also send to mobile phone.



4. CONCLUSION

The biggest threat lies with susceptibility of the pin entry process to direct observational attack, such as human shouldering and camera based recording. As per our motive technique bank server will accept PIN from users mobile phone and not from merchants keypad. This will help user to secure his PIN number to become public. Different type of pattern will increase users PIN security and those patterns can change on daily or monthly basis. The Main aim of this system is to help users in performing their transactions in more secure way also we provides a security for digital transaction by implementing card payment system along with permission of authorized device. This help to prevent shoulder surfing attack with the concept of concealing the password object information

which is applicable for all Electronic payment system. We provide security by forcing user to enter his password directly by performing certain mental task to drive indirect correct password.

REFERENCES

1.] Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks, IEEE 2014 Taekyoung Kwon, Member, IEEE, and Jin Hong- IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY

2.] International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014 Credit Card Fraud Detection System Using Hidden Markov Model and K-Clustering

3.] Lee, Mun-Kyu. "Security notions and advanced method for human shoulder surfing resistant PIN-entry." Information Forensics and Security, IEEE Transactions on 9.4 (2014): 695-708

4.] De Luca, Alexander, et al. "Using fake cursors to secure on-screen password entry." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2013.

5.] Credit Card Fraud Detection System Using Hidden Markov Model and KClustering. MohdAvesh Zubair Khan, Jabir Daud Pathan, Ali Haider Ekbal Ahmed. International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014

6.] A PIN Entry Method Resilient Against Shoulder Surfing. Volker Roth, Kai Richter. Rene Freidinger Technical University Darmstadt Germany