International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

A Novel Approach of Card Payment to avoid Overlooking & Shoulder Surfing Attacks

Jyoti Chikane
jyoti.chikane999@gmail.com
SP'sInstitute of Knowledge College Of Engineering
Gaikwad Priyanka
priyagaikwad7795@gmail.com
SP'sInstitute of Knowledge College Of Engineering
Funde Kishor
mailmekishor.funde@gmail.com
SP'sInstitute of Knowledge College Of Engineering
Prof.Ritesh Thakur
hod_comp_iok@yahoo.com
SP'sInstitute of Knowledge College Of Engineering, Department of computer engineering, Savitribai Phule University.

Abstract:

A chip is a small microchip embedded in your credit card. It is encrypted so transactions are more secure on the card. The Chip+ PIN card is a superior level of security on your card, in line with best global practice 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. We suspect a security thread in this process. While providing PIN in front of friends, relative or unknown person, it is affected by "Shoulder attack". Shoulder attacks is one of the latest weapons used by hackers or adversaries in an organization to hack an account or to authenticate in a secure zone. In a shoulder attack a person is watching the user while he is typing the password and reads his fingers that what he has typed or makes a video of him typing the password and so comes to know that what the password is. We wanted to address this problem. So to handle such type of attacks we wanted to developed such a technique which provides more security to a user in typing his password, in a public place, and in case that user is in critical position. As per our propose technique we wanted bank server should accept PIN from users mobile phone and not from merchants keypad.

Keywords: Shoulder Surfing; Authentication; Security; SS7.0; Shoulder Attacker; password entry

Introduction:

The flow of Card Payments are changed in recent months (OCT 2014) and made PIN number compulsory to complete the transactions. This is applicable for all types of cards (Debit, Credit, etc).This is done to minimize the fraud/misuse of card payments. A Novel Approach of Card Payment is to avoid Overlooking & Shoulder Surfing Attacks. So when ever merchant swap user card for payment, bank server will notify user on his mobile to enter PIN number. User can now enter PIN using his/her mobile. Even user is free to provide

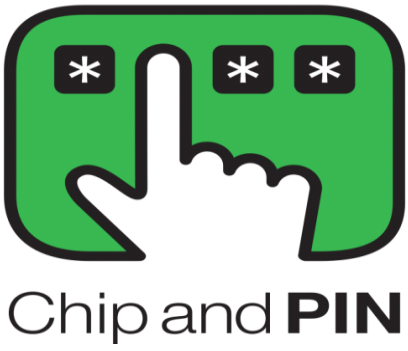
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

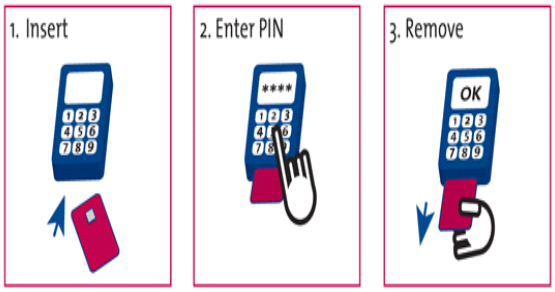
number as YES/NO or any pattern which he can change on daily or monthly basis.

Problem Statement:

- We found a problem when user is typing his/her PIN number.
- He / She has to enter PIN in front of merchant or relatives or any other person.
- This is a type of **Overlooking / Shoulder Attack.**

Existing System:





The card payment is also affected by same attack. If we look into STEPS of card payment:

Step1: The merchant inserts your card at a PIN enabled POS terminal

Step2: He enters the transaction amount

Step3: The machine prompts for a PIN to be entered by you

Step4: You enter your Credit Card ATM PIN in the machine

Step5: On entering the correct PIN the transaction is confirmed and completed

Step6: For terminals without PIN authentication support, your new Chip+PIN credit card shall continue to support the regular signature mode.

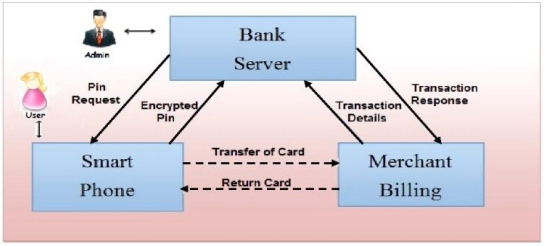
Disadvantages of Existing System:

- Frauds are increases when we type PIN on merchant machine.
- No security.

Proposed System:

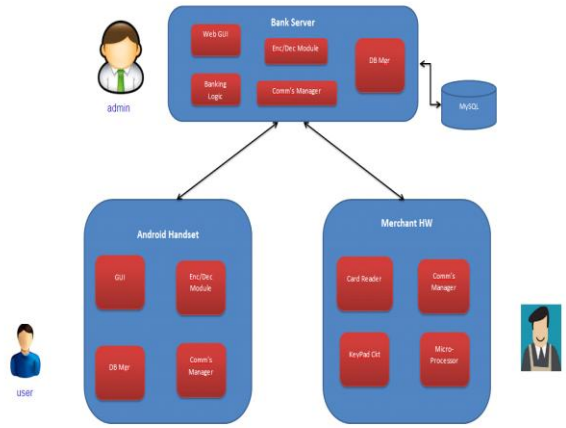
In step no 5, we have entered PIN in front of merchant or friends to complete transaction where those people can remember my PIN number. So to handle such type of attacks we wanted to developed such a technique which provides more security to a user in typing his password, in a public place, and in case that user is in critical position. As per our propose technique we wanted bank server should accept PIN from users mobile phone and not from merchants keypad. So when ever merchant swap user card for payment, bank server will 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 will be using AES/DES security system for communication between bank server, mobile application and Merchant hardware.



Architecture of Card Payment

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org



Hardware Interfaces:

- Processor – Intel Core2Duo, Pentium – III/i3
- Speed – 2.4 GHz
- RAM - 1 GB (min)
- Hard Disk - 50 GB

- Android 2.3 enable handset
- Card Reader

Software Interfaces:

- Operating System : Windows 7
- Front End : Java 7
- Back End : MySQL 6
- Tomcat 7
- JDK 1.7
- Android SDK
- Eclipse Indigo

Advantage:

- More secure in typing PIN no.
- We can set our own pattern of providing PIN no.
- One can now share card with our friends/relative because he is only going to enter PIN remotely
- Will minimize fraud cases
- Can Easily Integrate with existing system.

Acknowledgement:

We express our sincere and profound thanks to all our teachers. We wish to thank Prof. Ritesh Thakur (guide) for his student-like enthusiasm and his guidance from time to time. We heartily thank for all his help and valuable time. His invaluable advice has helped us bring this work to completion.

Conclusion:

In this paper, we minimize the fraud/misuse of card payments. The main motive behind implementing this project is avoid the shoulder attacks.

References:

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

[2] International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)ISSN: 0976-1353 Volume 13 Issue 1 –MARCH 2015. PREVENTING HUMAN SHOULDER SURFING AND TO PROVIDE RESISTANCE AGAINST PIN ENTRY.

[3] 2010 IEEE Symposium on Security and Privacy Chip and PIN is BrokenSteven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond University of Cambridge Computer

Laboratory Cambridge, UK http://www.cl.cam.ac.uk/users/{sjm217,sd410,rja14,mkb23}.

[4] ColorPIN – Securing PIN Entry through Indirect Input Alexander De Luca, Katja Hertzschuch, Heinrich Hussmann Media Informatics Group, University of Munich, Amalienstr. 17, 80333 Munich, Germany {alexander.de.luca, heinrich.hussmann} @ifi.lmu.de,hertzschuch@cip.ifi.lmu.de.

[5] IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. II (Jan – Feb. 1) 2015), PP 58-65 www.iosrjournals.org DOI:10.9790/0661-17125865 www.iosrjournals.org 58 | Page Moving ATM Applications to Smartphones with a Secured PinEntry Methods Kavitha V 1, Dr. G. Umarani Srikanth 21,2,(Department of PG studies, S.A. Engineering College, India).

[6] Hindawi Publishing Corporation Scientific World Journal Volume 2014, Article ID 838623,12 pages http://dx.doi.org/10.1155/2014/838623 Research Article Preventing Shoulder-Surfing Attack with the Concept of Concealing the Password Objects' Information.