

A Survey on “Security of smart card payment”

TawareTushar , BhosaleAmit , SurveSujit

Department of Computer Engineering
Someshwar Engineering College, Someshwarnagar,
tushar.taware24@gmail.com, amitraje96k@gmail.com,
surve7sujit@gmail.com

Abstract: Shoulder surfing uses direct observation techniques, such as looking over someone's shoulder for information. It is an effective way to get information in crowded places because it is relatively easy to be next to someone who enters a PIN number. When the customer hits his credit / debit card at the merchants terminal then the merchant system will communicate with the bank server for the bank server clients for the bank account details of the customers. The bank server will also notify customers of the mobile phone to enter the PIN and the customer will enter their pin from their mobile phone instead of the merchant's keyboard. To ensure communication between the banking server and the client, they will use security algorithms such as the Brute Force algorithm, the MD5 Hashing algorithm and the Base64 algorithm. There proposed technique will ensure the flow of payment of the card.

Keywords: User Authentication, Shoulder Surfing Attack, Personal Identification Number, Session Key.

Introduction

Today, one of the weapons of hackers is the shoulder attack. It is used to hack confidential user information such as financial records, bank account passwords. In a shoulder attack an attacking person is viewing the user while typing the password and reads their fingers than what he has written for password acquisition. They wanted to address this problem. To handle these types of attacks, they wanted to develop a technique that would offer

more security to a user by typing his password, in a public place such as shopping centers, cinemas, etc. The systems use the CHIP + PIN method. Activated CHIP + PIN credit cards offer more security and protection against fraud. According to there proposal technique they wanted bank server to accept PIN from mobile phone users and not keyboard merchants. Therefore, when the user card swap user payment, the bank server will notify user on their mobile to enter the PIN number

Technical Methods

Black and white method:

The basic model consists of the horizontal digits from 0 to 9 and randomly arranged colors. The black and white method divides 10 digits into two halves, is played when the user with the TM application mobile service. Black and white method is selected from. According to the user's key entry in Each round B & w method consists of four iterations. Each iteration refers to the pin entry of a single pin.

Traditional System

- To carry out literature survey on existing system
- First of all the merchant take the user card and then swap into the machine.
- Then after swapping the card merchant will ask user to enter the pin into swap machine.
- When user enter the pin into swap machine that time 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

- To handle such type of attacks they want 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 there propose technique they wanted bank server should accept PIN from users mobile phone and not from merchants keypad.

Related Work

A. Guessing Attack

In a guessing attack (GA), the attacker guesses a user's PIN and inputs it to pass the test. A smart attacker might use the fact that the distributions of PINs and passwords are not uniform [10]–[12]. However, to simplify analysis, they make an idealized assumption that the distribution of PINs is uniform. They also have to take into account that the user (and the attacker) may be allowed to fail several times until s/he inputs the correct PIN. For example, atypical ATM permits three trials. Therefore, they give the following definition for the security of a PIN-entry method against a guessing attack.

B. Shoulder Surfing Attack (SSA)

In a shoulder-surfing attack, the attacker observes the logon procedure by looking over the user's shoulder, and tries to recover that user's PIN. The strongest variant of this attack is a recording attack (RA), in which the attacker employs a recording device to record the entire authentication recording session. Let us call an attack without any recording device a human shoulder-surfing attack (HSSA).

Proposed System

From the above mentioned payment system, they have entered the PIN in front of the merchant or friends to complete the transaction where those people can remember my PIN number. Therefore, to handle this type of attacks, they want to develop a technique that provides a user with more security when entering his password, in a public place and in case the user is in a critical position. According to

there proposal technique they wanted bank server should accept PIN from users mobile phone and not from merchants keypad. So whenever 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 you are free to provide number YES / NO or any pattern which I can change on daily or monthly basis. They will be using Encryption and Decryption security system for communication between bank server, mobile application and Merchant hardware.

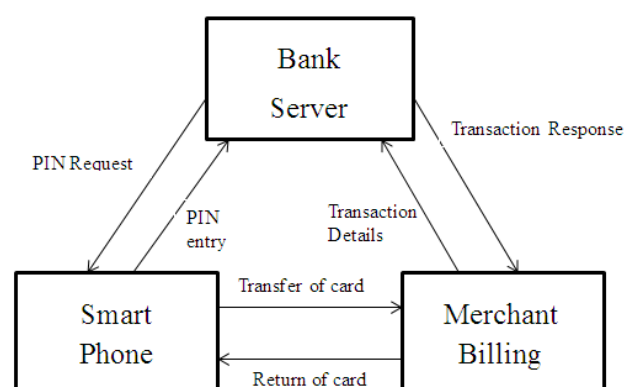


Fig 1: Architecture of Card Payment Security

Architecture:

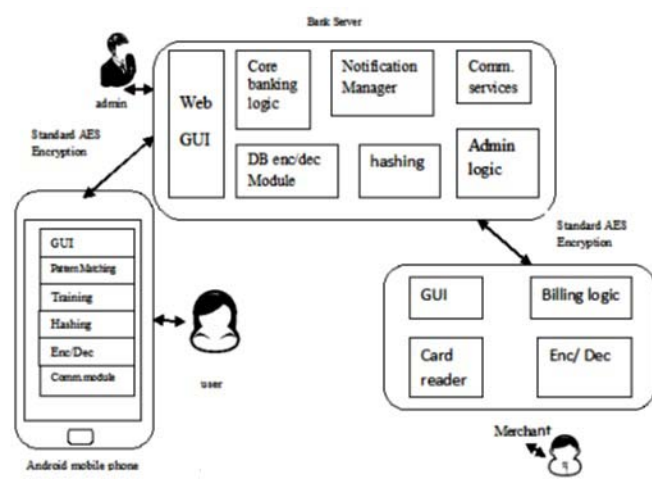


Fig 2: Architecture of Card Payment

1. Keypad Circuit:-

The keyboard circuit will provide numeric keypad to write a quantity.

2. Communication Manager:-

Communication Manager will manage the communication between the client side and the server side.

3. Web GUI:-

This means that most of the logic runs on the server side.

4. Banking Logic:-

Banking logic will handle the payment and transactions.

5. Card Reader:-

Card reader will scan a card.

6. Database Manager:-

Database manager manages the database of the system.

7. System Configuration:-

System configuration handles all the configuration files of the system.

8. Encryption/Decryption Module:-

This module will handles all encryption and decryption logic.

Algorithm:**1. Brute Force Algorithm:**

This algorithm is used to match the input PIN pattern. Requires a verification algorithm after a possible match to verify if a true match occurs. In the preprocessing phase, the complexity of space and time is $O(m)$. In the search phase, the complexity of time is $O(n + m)$, where n is the length (size) of the file and m is the length of the pattern.

2. Base64:

It is a group of similar binary-to-text encoding schemes that represent binary data in an ASCII string format. When translating it into a radix-64 representation. The general strategy is to choose 64 characters that are members of a subset common to most encodings, and also printable. The particular set of 64 characters chosen to represent the 64 place values for the base varies between

implementations. The ratio of output bytes to input bytes is 4: 3 (33 overhead). Specifically, given an input of n bytes, the output will be $4/3$ bytes long, including fill characters. They use this algorithm to encrypt the password of the users that is stored present in the database of the server.

3. MD5 hashing:

Production of a 128-bit (16-byte) hash value, typically expressed in text format as a 32-digit hexadecimal number. They encrypt users who receive PIN using MD5 before sending that PIN to server. MD5 is a one-way function; It is neither encrypted nor encrypted. It can not be reversed except by a brute force attack. The input message is divided into blocks of 512-bit blocks (sixteen 32-bit words). The message is filled so that its length is divisible by 512.

Conclusion

A simple and efficient system has been developed that solves the problem under study. Card payment system security helps to solve the shoulder surfing attack and offers a simple solution to avoid the shoulder attack problem.

Reference

1. Taekyoung Kwon, *Member, IEEE*, and Jin Hong proposed a paper "Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks," in *Proc. IEEE transactions on information forensics and security*, vol. 10, no. 2, february 2015
2. Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", *International Journal of Soft Computing and Engineering (IJSCE)* ISSN: 2231-2307, Volume 2, Issue 3, July 2012.
3. Gayatri Kulkarni, Pranjali Gujar, Madhuri Joshi, Shilpa Jadhav, "Message Security Using Armstrong Numbers and Authentication Using Colors", *International Journal of Advanced Research in Advance Computer Science and Software Engineering* ISSN: 2277 128X, Volume 4, Issue 1, January 2014.
4. Rajalakshmi and V. Valarmathi Assistant Professor, "Preventing Human Shoulder Surfing and to Provide Resistance Against Pin Entry" *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)* ISSN: 0976-1353 Volume 13 Issue 1, March 2015.
5. Mun-kyu, "Security Notions and Advanced method for Human Shoulder-Surfing Resistant PIN entry", *IEEE Transactions on Information Forensics and Security*, Volume 4, No 4, April 2014

6. Justin Weaver, Kenrick Mock, BogdanHoanca from Compute science and Computer information systems proposed "Gaze-Based Password Authentication through Automatic Clustering of Gaze Points" in Computer security Proc IEEE 2011.
7. Daphna Winchell from School of Computer Science and Engineering, proposed paper "Cognitive Authentication Schemes Safe Against Spyware," In Proc. IEEE Symposium on Security and Privacy (S&P), May 2006.
8. Desney S. Tan, Pedram Keyani, Mary Czerwinski, proposed paper "Spy-Resistant Keyboard: Towards More Secure Password Entry on Publicly Observable Touch Screens," from Microsoft Research in 2000.
9. S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in Proc. AVI, 2006, pp. 177–184.
10. V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in *Proc. ACM Conf. Comput. Commun. Security*, 2004, pp. 236–245.
11. M. Backes, M. Drmuth, and D. Unruh. Compromising Reflections - or - How to Read LCD Monitors Around the Corner. In IEEE Symposium on Security and Privacy, May 2008.
12. SMETTERS, D. K., AND GRINTER, R. E. Moving from the design of usable security technologies to the design of useful secure applications. In Proceedings of the New Security Paradigms Workshop (Virginia Beach, VA, USA, Sept. 2002), ACM, pp. 82–89.
13. B. E. John and W. D. Gray, "CPM-GOMS: An analysis method for tasks with parallel activities," in *Proc. ACM SIGCHI Conf. Human Factors Comput. Syst.*, 1995, pp. 393–394.