Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

SteganoPIN – A secured PIN for ATMs

[1]Kaavya, [2]Kamalini, [3]Hemalatha and [4]Dr.Sandra Johnson
[1,2,3,4]Department of Information Technology, R.M.K. Engineering College, TamilNadu, India

***Abstract*—**Users mostly reuse their same personalized identification number (PIN) for multiple systems and in numerous sessions. Direct PIN entries are highly susceptible to shoulder-surfing attacks where the attackers can easily observe PIN entry with concealed cameras. Whereas, Indirect PIN entry methods acts as a countermeasures which are rarely deployed because they demand a complex intellectual activity workload for users. To achieve security and usability, practical indirect PIN entry method are used and they are called SteganoPIN. The human–machine interface of SteganoPIN consists of two numeric keypads which as a covered one and the other is the open one, these are designed physically to block shoulder surfing attacks. The two keypads: static and challenged *(or)* shuffled key pads; the challenged keypad can be seen only if the proximity sensor senses the user's cup-shaped hand gesture. After locating the PIN in the keypad layout, through the covered keypad, a user generates a one-time PIN that can safely be entered in plain view of attackers. This enables the user to establish a secure transaction by means of a mobile application to the server by implementing the SteganoPIN method using invisible keypad and colorpin concepts that are based on independent PIN entry system (Standard PIN, SteganoPIN).

Keywords*—Steganograhy; shoulder-surfing attack; security; ATM;*

I. INTRODUCTION

The great threat for the user who is performing the bank transaction is the shoulder surfing attack. These attacks are very common in the over populated area. In order to overcome this attack many methods and techniques are proposed. In spite of these methods the attackers are intelligent to find the counter measures[1] . So, The main objective of this paper is to propose a practical indirect PIN entry technique called SteganoPIN where The human–machine interface of SteganoPIN is two numeric keypads, one covered and the other one is opened, which are designed to physically block shoulder surfing attacks. To establish a secure transaction between the mobile Application and Server by implementing the SteganoPIN and improved BW method. Personal identification numbers (PINs), typically constructed and memorized, is widely used as numerical passwords for user authentication or various unlocking purposes[2]. Their application is increasing because modern touch screens can facilitate convenient implementation of the PIN entry interface on a variety of commodity machines and devices, including Automated Teller machines (ATMs), point-of-sale (POS) terminals, debit card terminals, digital door-locks, smart phones, and tablet computers.

Kavitha V. and Dr. G. Umarani Srikanth in 2015 [3] proposed a method that uses the PIN entry methods which offers protection against such attacks. The PIN entry methods that are used in this system include invisible keypad and improved black–white method. The main aim of the proposed system is to create an android application which performs the ATM cash transactions that can be connected to the smart phones. The concept of virtual money is used. The hash function is used to send the PIN securely through the public channels guessing attack (GA), where the adversaries guesses a user's PIN and inputs it to pass the test. An adversaries might use the fact of non-uniform password or PIN distribution. The account of the user should be consider, which results in failure after several attempts until they succeeds in entering the correct PIN. For example, a typical ATM permits a maximum of three trials. Therefore, the following protocol for the proposed security of a PIN-entry method is said to deter the adversaries from succeeding in their guessing attack.

SteganoPin system is used to address the camera-based shoulder-surfing attacks by multiple authentication and to migrate the users already known with the standard steganoPin entry system. The SteganoPIN system is constructed on the concept of challenge and response rendered over a user interface [4], [5] and physical hand protection [6], [7] to advance the following goals for PIN-based authentication.

1. Usability: Must use the regular numeric keypad (which is called as response keypad) for key entry. should incur limited increases in PIN entry time and error rates. It should not rise the length of a long-term PIN. Should be below the short-term memory requirements of human limitations, such as four groups of items [8], [9].
2. Strong Security: Should be against the camera-based shoulder surfing attacks over multiple authentication sessions. Must resist active guessing attacks without allowing more advantage than random guessing[10].

II. LITERATURE REVIEW

In Greek, the word Stegano pin means concealed or protected. In this system, the numeric keys entered by users in plain view of the attackers must be one-time PIN (OTP) keys that protect a real PIN following instant derivation. To make such a derivation process easy for users, we use a two-faced keypad system, which means a novel user interface with two numeric keypads. To make such a derivation process secure against attackers, we incorporate a human–machine interactive protection method.

In an existing system, when a user directly enters a secret PIN into such systems, security is easily compromised, particularly in public places. The camera-based shoulder-surfing attacker is defined as a stronger adversary assisted by an automatic recording tool, such as a wearable camera, to record and analyze entire transactions effectively even at long range . When a user enters a personal identification number(PIN) as a numeric password in any of the electronic gadgets which includes mobile phones, smart phones tablet computer and automated teller machine(ATM), and point of sale (PoS) terminals, a direct observation attack some attacks on shoulder surfing has great concern. The pin entry is observed by nearby adversaries, more effectively in a crowded place. Since the same PIN is usually chosen by a user for various purposes and, a compromise of the PIN may be of great risk.

III. PROPOSED SYSTEM

In the proposed system, the framework called Steganopin entry method for secure pin authentication system for ATM using Smart Mobiles. The Steganopin authentication which can be done by the user mobile. A Smartphone to sense both proximity and touch events on the challenge keypad and the normal keypad For OTP derivation. For steganopin authentication, the user has to close cups a hand on the circle with the grip circularly closed in a ρ-shape[10]. Inside that, the user will see

the random shuffled keypad, and then the user locates a PIN in regular keypad and subsequently maps the key locations into the random shuffled keypad for OTP derivation. The user then enters the OTP on a regular keypad called the response keypad.

The BW method is proposed ,by improving the BW method which have been used before, in this the proposed algorithm uses randomly generated four digits in which each digit block, is combined with the combination of two, to avoid the attentional shoulder surfing attacks by generating the PIN digits after all the user iterations got completed[12]. Another possibility is to keep the numeric keypad in the regular layout, but produce many combination pins by generating the OTP, so that the adversary is frustrated. The adversary who launches covert attentional shoulder surfing need to know four color groups and attend to one of them for the next round, while the user only needs to answer either of the two colors that fill his/her PIN digit key in each round[13]. Authentication Services are also provided by this method.

There are four modules used in the proposed system,

1. User Registration
2. Improved BW method
3. SteganoPIN Authentication
4. Banking and Services

A. User Registration

User Registration is done through this application and the user is able to access the ATM application in their mobile phones. Once the User complete their registration process , they will be provided with a Unique PIN, which is OTP, Sent to their registered Mail ID. Once it got validated a User will be able to access our Application by entering the Username and Password Chosen at the time of Registration.

B. Improved BW method

In this Method ,a new Strategy is implemented which will completely avoid the Shoulder Surfing attacks even the adversary is from the Well Trained Perceptual Group, they could not Crack the PIN Digit Entered by the User in a Conventional Way. Let A denote a set of four colors and(or) patterns customizable. Here A = {black, red, white, blue} or P = {black, white, dotted, diagonal stripes}, for a color blind person. Therefore, the improved technique runs as follows: The system displays a set of ten digits, P = {0, ???, 9}, on the response numeric keypad with two split colors(say upper or lower color), chosen from A, in each numeric key; and the four color keys below. A color is chosen at random from A and fills five random splits of distinct keys. The remaining colors fill five splits, respectively, in the same way. The user attends the PIN digits and enters either of its color through the color key. The user and the color system repeats this methods for m rounds that the PIN digit is identified by intersection, and until the entire PIN digits are identified.

C. Stegano PIN System

A prototype system of SteganoPIN to simulate a horizontal ATM interface with a Smartphone (to sense both proximity and touch events on the challenge keypad) and a tablet (to implement the response keypad), For OTP derivation.

The challenge keypad does not appear immediately. Only the response keypad appears in its regular layout and size. It shows the challenge keypad only when a user cups a hand on the circle with the grip circularly closed in a ρ-shape. The challenge keypad then shows up after a small delay and disappears immediately when the user releases the cupped hand.

The user interface of SteganoPIN, one numeric keypad is a standard keypad in regular layout and the other is a small separate keypad in a random layout. The random layout keypad is called the challenge keypad because it permutes ten numeric keys as a random challenge, as in. A user must use this challenge keypad to derive a fresh OTP. The user first locates a long-term PIN in regular layout and subsequently maps the key locations into the challenge keypad for OTP derivation. The user then enters the OTP on a regular layout keypad called the response keypad. The procedure can be repeated if the PIN length.

D. Authentication & Services

Once the User Entered Pattern is manipulated and a PIN is Identified, It will be checked with the Local Database provided by Android OS using SQL Lite. This Process is used to prevent the unwanted Server and process handling playful requests. A One Way Hash is generated for the Validated PIN and is sent to Server in public channel so that an active attacker cannot take away the PIN by monitoring the channel. Once got Authenticated by Server a Quick Response to the Mobile App will redirect the user to the Services. In ATM Services Cash transactions like Withdrawal, Deposit and Fund Transfer can be securely done by using the concept of Virtual Money which is employed by many other Applications Successfully in the Web. This reduces the overhead complexities in the server and will provide the User an ease of access to the Banking Services.

CONCLUSION

The security of our method relied on such a physical hand protection process. Although it was easily and safely enforced by users, an overhead-installed camera remained a concern in a very few cases, depending on a user posture. Moreover, a simplified hand shape may reduce the security of the system, depending on the place of the circular touch area. For implementation, it would be desirable to place the circular touch area as close to the user as possible. Thus, in general, the SteganoPIN system is more appropriate to stationary systems, such as ATM and PoS terminals, than mobile systems although it can be provided as a promising option for mobile system users who want to choose stronger security in a public place. In future,the work can be extend to process the other bank-account transactions and to achieve further reduction in the time consumption.

References

[1] T.Kwon,S.Shin,andS.Na,"Covert attentional shoulder surfing: Human adversaries are more powerful than expected,"IEEE Trans.syst.,Man,Cybern.,Syst.,vol.44,no.6.,pp.716-727,Jun 2014.

[2] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in Proc. ACM Comput.Commun. Security, 2004, pp. 236–245.

[3] Kavitha V, Dr.G.Umarani Srikanth "An Android Application For ATM With A Secured Pin-Entry Methods" International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397 Vol. 7 No.4 Apr 2015

[4] T. Matsumoto and H. Imai, "Human identification through insecure channel," in Proc. Adv. Cryptol., 1991, pp. 409–42.

[5] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. W. Nicholson, J. Nicholson, and P. Olivier, "Multi-touch authentication on tabletops," in Proc. ACM SIGCHI Conf. Human Factors Comput. Syst., 2010, pp. 1093–1102.

[6] Q.Yan, J. Han,Y. Li, J.Zhou, andR.H.Deng, "Designing leakage-resilient password entry on touchscreen mobile devices," in Proc. 8th ACMSIGSAC Symp. Inform., Comput. Commun. Security, 2013, pp. 37–48.

[7] T. Kwon and S. Na, "SwitchPIN: Securing smartphone PIN entry with switchable keypads," in Proc. IEEE Int. Conf. Consumer Electron., 2014, pp. 27–28.

[8] N. Cowan, "The magical number 4 in short-term memory: A reconsideration of mental storage capacity," Behavioral Brain Sci., vol. 24, no. 1, pp. 87–114, 2001.

[9] G. A. Miller, "The magical number seven, plus or minus two: Some limits on our capacity for processing information," Psychol. Rev., vol. 101, no. 2, pp. 343–352, 1956.

[10] Q. Yan, J. Han, Y. Li, and R. H. Deng, "On limitations of designing leakage-resilient password systems: Attacks, principles and usability," in Proc. 19th Internet Soc. Netw. Distrib. Syst. Security Symp.,2012, pp. 1–16

[11] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected," IEEE Trans. Syst., Man,Cybern., Syst., vol. 44, no. 6, pp. 716–727, Jun. 2014.

[12] T. Perkovic, A. Mumtaz, Y. Javed, S. Li, S. A. Khayam, and M. Cagalj, "Breaking undercover: Exploiting design flaws and nonuniform human behavior," in Proc. 7th Symp. Usable Privacy Security, 2011, pp. 1–15.

[13] A. De Luca, K. Hertzschuch, and H. Hussmann, "ColorPIN–Securing PIN entry through indirect input," in Proc. ACM CHI Conf. Human Factors Comput. Syst., 2010, pp. 1103–1106.