ENSHROUDING OF PIN FROM SNOOPING USING STEGANOPIN AND BW METHOD

M.Swaminathan[1],JaavajiAshok[2], V.Santhosh[3], V.D.Ambeth kumar[4] , M.Rajendiran[5]
Department of computer science
Panimalar Engineering College,
Chennai, TamilNadu.
Mail Id: santhoshvinayagamurthy@gmail.com, sathish.msathish.sathish@gmail.com, ashok99.j@gmail.com

Abstract:

Now a daysUsers typically reuse the same personalized identification number (PIN) for multiple times. Direct PIN entries are highly dangerous for shoulder surfing attackers can effectively observe PIN entry with hidden cameras. Indirect PIN entry methods proposed as countermeasures are rarely deployed because they demand a heavier brain stuff workload for users. To achieve security and usability, we present a practical indirect PIN entry method called SteganoPIN.

The human–machine interface of SteganoPIN is two numeric keypads, one which is covered and the other open, designed mainly to block shoulder-surfing attacks. After locating a long-term PIN in the more typical layout ,through the covered permuted keypad, a user generates a one-time PIN that can safely be entered in plain view of attackers. Forty-eight participants were involved in investigating the PIN entry time and error rate of SteganoPIN. Our experimental manipulation used a within-subject factorial design with two independent variables: PIN entry system (standardPIN, SteganoPIN) and PIN type (system-chosen PIN, user-chosen PIN).The PIN entry time in SteganoPIN (5.4–5.7 s) was slower but acceptable, and the error rate (0–2.1%) was not significantly different from that of the standard PIN.

Keywords: steganopin ,bw method ,shoulder surfing

1. Introduction

Personal identification numbers (PINs), typically constructed and memorized, is widely used as numerical passwords for user authentication or various unlocking purposes. 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.

In an existing system, when a user directlyenters a secret PIN into such systems, security is easily compromised, particularly in public places. The camera-based shoulder-surfingattacker 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 mobile or stationary systems, including smart phones, tablet computers, automated teller machines (ATM), and point of sale (PoS) terminals, a direct observation attack based on shoulder surfing becomes great concern. The PIN entry can be observed by nearby adversaries, more effectively in a crowded place. Since the same PIN is usually chosen by a user for various purposes and used repeatedly, a compromise of the PIN may cause the user a great risk.

The attacker can be standing in queue behind the authenticating person and looking at the PIN entry and execute a shoulder-surfing or observation attack.

The attacker may also install a small camera on the top surface of the ATM terminal to record PIN entries of users at the point-of-service.

In the proposed system, the framework called Stegano pin entry method for secure pin authentication system for ATM using Smart Mobiles. The Stegano 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 stegano pin authentication, the user has to close cups a hand on the circle with the grip circularly closed in a ρ-shape. 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 procedure can be repeated until the PIN length

2. Literature Survey

Matsumoto et al. [1], 1991 proposes human identification through insecure channel that tells about the new problem of relatively how to securely identify a human through insecure channel, it seems to be simple but it is a powerful cryptographic scheme that goes with human ability of memorizing and processing. Typical applications of this scheme are identification verification of user at on line through an equipment like automatic vendor machine. The main pros is that memory computational and communicational complexity acceptable for human proves and even for human verifier. Some of the cons are probabilities of someone might go wrong. Finally, the author concludes by saying apply the proposed system to the core and develop further more easier versions and moreover any one of the channel in which human receives a message and one sends message.

K. Richter et al. [2], 2004 suggests a new method of pin entry method that is resilient against shoulder surfing. The issue that is to be ruled out by this scheme is that shoulder surfing and through miniature cameras. The author brings here the new approach called “cognitive trapdoor” method in which the criminal cannot even guess the user’s pin even when we are tracking the

full usage of pin. This is the main positive fact that user only knows what number he has typed. Some disadvantages also there but the safety of this scheme will override cons. The number of rounds of pin entry is more compared to regular pin entry methods. The author also emphasize the immediate oracle method which reduces the execution time in higher weariness.

D. Weinshall et al. [3] 2006, suggested the cognitive authentication schemes safe against spyware. This scheme will avoid problems like eavesdropping adversaries based on human function alone. Here the author tells about the challenge response protocols based on shared key set of pictures. Brute force attacks are key restraint of eavesdropping. Success rate of this scheme is about 95%. Some disadvantages is that it took slight delay on high complexity protocols. Also author has described challenge response authentication protocols, based on the user's nature cognitive abilities.

A.De Luca et al. [4], In 2010 With increase of ATM machine frauds new authentication mechanisms developed to overcome security problems of Personal Identification Number. A field study says that there is a big influence of contextual factors on security and performance. From these findings we draw several implications for design through resilient distraction and social compatibility.Social compatibility authentication even in distractive environments. It has only limited validity to other cultural area. Some studies suggests that ATM s cannot rely on user but needs security features which are built in into authentication mechanism. This represents the first step in uncovering ATM use in wild, hopefully helping to gain a broader insight on real factors and constraints of ATM authentication.

H.J. Asghar et al. [5], In 2010 In this we show two probabilistic attacks which reveal user's secret after observation of only a handful of authentication sessions.

This convex hull can be performed by humans without additional aid. It is based on a security of the convex hull based protocol of secret icons in a set of graphical icons and then clicking randomly within this convex hull.Lack of an explicit expression for p(m,k,r), the success probability of attack .Demerits is impersonation, geometric problems .Convex Hull Click graphiacal human identification protocol is an interesting alternative to other proposed protocols in literature. Our approach has been as mathematically as rigorous as possible.

Alexander De Luca et al, [6], In 2009 defined a new concept called vibrapass. The vibrapass concept basically targets on observed attacks which are very familiar in atm or in internet transaction its helps us to prevent shoulder surfing attacks .it prevents informal recording of the passwords. Vibrapass uses tactile feedback to resist from the attacks . One Time Password (OTP) is shared between the mobile and the terminal. It encrypts to the input it is very difficult for the observer to find the input .The advantages in this method is that it provides low error rates and fast inputs .It provides reasonable input speed at the low rate is the disadvantage .

David Kim et al. In 2010 [7] designed a modal that focus on tabletop interfaces which are very prone to shoulder surfing attacks .he proposed many authentication schemes one them is

multitouch interaction . The most shared interfaces has to differentiate between the user .The interfaces should remain to a particular user for a particular amount of time. It may be considered as a demerit sometimes because in case of any urgency also the object will not be allowed to the other user until the session is over .Tabletop users authentication takes place in front of number of observers. So we introduce and evaluate a many of tabletop authentication schemes.

Andrea Bianchi et al. [8], proposed a system in 2011 which prevents the hacking of the password in public places .The authentication is made using pin or passcodes that depends on the unobservable tactile or audio cues .spinlock is methodology proposed by the author. It has high load of cognitive loads in terms of processing, mapping or recalling non visual information. To solve this issue Spinlock, authentication technique used. The complexity of the previous system is avoided .The authentication with Spinlock is faster and less error prone than previous non-visual systems. Demerits in this system is that the latency of the haptic cues should be handled properly.

Toni Perković et al. In 2011[9] introduced a idea to deal with the undercover attacks and to find the non uniform behaviour. Its describes about the design flaws present in the system and these gives the high probability in finding passcode. A sensitive computer starts its authentication where the user has to provide its identity like biometrics, fingerprints etc. It gives some improvement to make undercover more secure .Breaking the undercover operation is of two types security related human computer interface and its explains about the relationship between the security and usability .It gives ideal way to deal with the security of the system .

Andrea Bianchi et al. In 2011 [10] invented the methodology which deals with the tangible user interface. A tangible user interface (TUI) is a user interface in which a person interacts with digital information using the physical environment. The initial name was Graspable User Interface, which is no longer used. when doing transaction in a public place many attacks can happen to steal the password .

These can be solved use the audio and the haptic cues .These non visual pin are less affected by the observation attacks .Studies showed the feasibility of the concept in terms of task completion time, error rate and user acceptance .Demerits are to find in other combinations of PIN . Tactile method provides the ability of securing the tangible interface in such system have to enter pin in the physical interface it does not have any graphical display

3.Existing

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 mobile or stationary systems, including smart phones, tablet computers, automated teller machines (ATM), and point of sale (PoS) terminals, a direct observation attack based on shoulder surfing becomes

great concern. The PIN entry can be observed by nearby adversaries, more effectively in a crowded place. Since the same PIN is usually chosen by a user for various

5. Proposed Method

We propose improved BW method by extending BW method, in which our proposed algorithm uses randomly generated four digits in which each digit block, is combined with the combination of two, to prevent the attentional shoulder surfing attack by extracting the PIN digit after all the user iterations got completed.

Another possibility is to keep the numeric keypad in the regular layout, but produce more perceptual groups so that the adversary is frustrated

The adversary who launches covert attentional shoulder surfing may need to perceive 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. Authentication Services are also provided by this method.

The user has to register before accesing the system, and the user's data will be stored in the server. User has to click the corresponding link which has been sent to the user's mail for confirmation. User has to login with mail id and One Time Password (OTP), will be sent to the user. There are two methods of authentication, the user has to select one out of them. Two methods of authentication are Steganopin and Improved BW method.

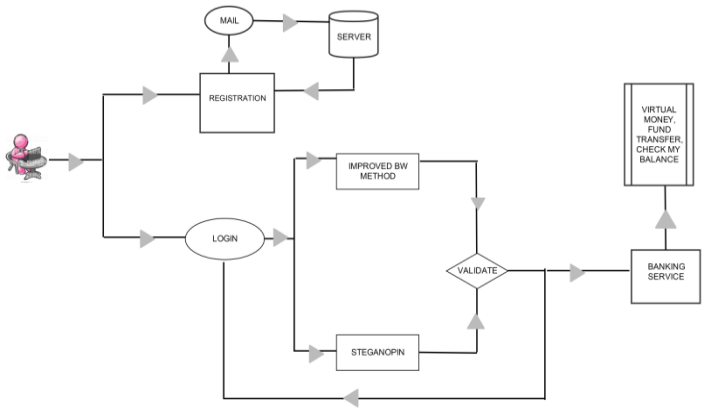

Fig :5.1 Shows the architecture of the proposed system

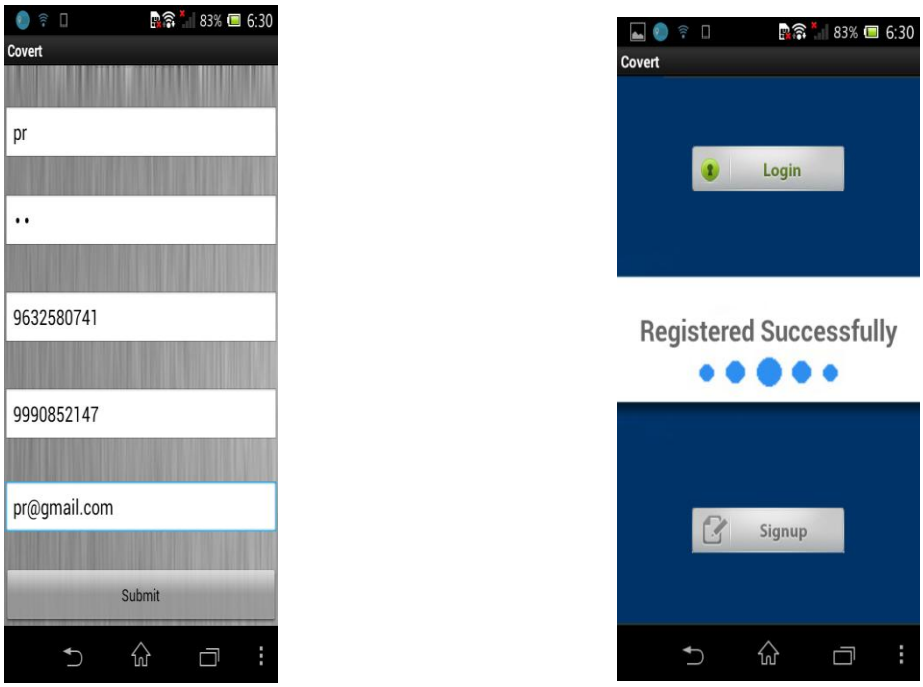

FIG 5.2 user registration

Modules:

1. User Registration

2. Improved BW method

3. SteganoPIN Authentication

4. Banking and Services

User Registration

User Registration is done and after that the user is able to access the ATM application in their mobile phones. Once the User Registration is Complete, User will be provided with a Unique PIN Sent to Their Respective 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. Only one number is allowed to register, more than one number is not allowed for same mail id.

IMPROVED BW METHOD

In this process we propose a new Strategy that will completely neglect Shoulder Surfing and even a Well Trained Perceptual Grouper could not Crack the PIN Digit Entered by the User in a Conventional Way. Let Pdenote a set of four colors and/or patterns customizable. Let P= {black, blue, white, yellow} or P= {black, white, dotted, diagonal stripes}, for a color blind person. the developed method runs as follows: The system displays a set of ten digits, A = {0, ???, 9}, on the

regular numeric keypad with two split colors, chosen from P, in each numeric key; and the four color keys below. A color is chosen at random from Pand fills five random splits of distinct keys; each split could be either upper or lower one. The remaining boxes splits into five colours, in the same way the user attends to the PIN digit and enters either of its color through the color key. The user and the system repeat this procedure for m rounds the PIN digit is identified by interaction between the digits, and until the entire PIN digits are identified.

SteganoPIN 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 afresh OTP. The user first locates a long-term PIN in regular layout and subsequently maps the key locations in to 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.

AUTHENTICATION AND 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 to prevent unwanted Server end 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 extract 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 Withdrawal, Deposit and Fund Transfer can be done securely using the concept of Virtual Money which is already employed by many other Applications Successfully in the Web. This

6. Results and Discussion

Table .1 Comparison of exixting pin entry and proposed steganopin &bw method

Types of parameters	Existing method	Proposed method	Percentage reduction%
Pin entry in atm	Can be exposed in cameras	The password hacking Reduce	**75%**
Pin entry in the mobile /laptops	Prone to shoulder surfing or camera	The attacker cannot guess the pin	**100%**

7. Conclusion

The password Can entered more securely than the other pin entry.Systems.Shoulder surfing is minimized.

References

[1] T. Matsumoto and H. Imai, "Human identification through insecure channel," in Proc. Adv. Cryptol., 1991, pp. 409–421.

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

[3] D. Weinshall, "Cognitive authentication schemes safe against spyware," in Proc. IEEE Symp. Security Privacy, 2006, pp. 295–300.

[4] A. De Luca, M. Langheinrich, and H. Hussmann, "Towards understanding ATMsecurity—A field study of realworldATMuse," in Proc. ACMSymp. Usable Privacy Security, 2010, pp. 1–10.

[5] H. J. Asghar, S. Li, J. Pieprzyk, and H. Wang, "Cryptoanalysis of the convex hull click human identification protocol," in Proc. 13th Int. Conf. Inf. Security, 2010, pp. 24–30.

[6] A. De Luca, E. von Zezschwitz, and H. Hussmann, "Vibrapass – secure authentication based on shared lies," in Proc. ACM CHI Conf. Human Factors Comput. Syst., 2009, pp. 913–916.

[7]A. Bianchi, I. Oakley, and D. Kwon, “Spinlock: A single-cue haptic and audio PIN input technique for authentication,” in Proc. Haptic Audio Interaction Design, 2011, pp. 81–90.

[8] 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.

[9] A. Bianchi, I. Oakley, V. Kostakos, and D. Kwon, “The Phone Lock: Audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices,” in Proc. 5th Int. Conf. Tangible, Embedded, Embodied Interaction, 2011, pp. 197–200

[10] 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.

.