Secured pin entry method for ATM using steganopin and session key methods

S. Shanmuga Priya[1*], Ancy Breen W[1], V.S Rajkumar[1], Latha[2]
[1]Dept. of computer Science & Engineering, VelTech Hightech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, Chennai
[2]Department of MCA, VelTech Hightech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, Chennai
***Corresponding author: E-Mail: spriyavasan@yahoo.co.in**

ABSTRACT

Users typically reuse the same personalized identification number (PIN) for multiple systems and in numerous sessions. Direct PIN entries are highly susceptible to shoulder-surfing attacks as attackers can effectively observe PIN entry with concealed cameras. To achieve security and use ability, we present a practical indirect PIN entry method called SteganoPIN and Session key. The concept of SteganoPIN is two numeric keypads, one covered and the other open, designed to physically 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. SteganoPIN is resilient to camera-based shoulder-surfing attacks over multiple authentication sessions. It remains limited to PIN-based authentication. The concept of session key is an array of numbers and symbols arranged in the parallel manner. The entry system generates a one-time PIN that is send through a public network and validated.The main objective of the project is to create an android application for coping with shoulder-surfing attacks using multi-touch concept in SteganoPIN method. Only after the user PIN entered in the shuffled keypad matches with that of the static keypad, the authentication is then confirmed. Thus this method allows the user to perform a safe banking transaction through multi-touch SteganoPIN concept.

KEY WORDS: Authentication, personal-sized identification number (PIN) entry, security, 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 touchscreens 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. Unfortunately, when a user directly enters a secret PIN into such systems, security is easily compromised, particularly in public places. Nearby people can observe PIN entry by shoulder-surfing with or without concealed cameras (Long and Wiles, No Tech Hacking, 2008) (Greenberg, 2014). Ming Leietal proposed a virtual password concept involving only a minimum amount of human effort in creating a secure user's password in the online environment. It protects the user against phishing of the key logger and shoulder-surfing attacks.

The human-only shoulder-surfing attacker is defined as a weak adversary who has no automatic recording device, but may use manual tools such as a paper and pencil (Roth, 2004). The perceptual and cognitive capabilities of human-only attackers are confined to those of humans (Kwon, 2014). 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 (Greenberg, 2014). Moreover, adversaries who have already mounted shoulder-surfing attacks and collected multiple PIN candidates can attempt to impersonate a user. The active-guessing attacker is an adversary who attempts guesses with PIN candidates. Such an attacker can become more powerful when she repeats camera-based observation of the same user and system (Yan, 2012).

Remote connected observation is also becoming a concern because high-resolution cameras are being distributed and networked in public places (Parti and Qureshi, 2014; Song, 2012). The recent trend of targeting attacks and the advent of wearable computers make repeated camera-based shoulder-surfing attacks an increasingly realistic threat to the PIN user interface. The number of PIN candidates must remain sufficiently large to reduce information leakage even if a user's PIN entries are repeatedly observed by adversaries. Even partial information leakage could be harmful because users typically reuse identical or at least similar PINs for multiple systems. Furthermore, a token and/or ID often combined with a PIN can be pickpocketed or skimmed by adversaries using other physical channels (De Luca, 2010; 2007). Thus, once a secret PIN is compromised, a user could be exposed to multiple breaches of security.

Existing System: The existing system of the secure PIN entry methods have also concentrated on the shoulder surfing attacks. The list of existing methods says how important it is to provide security to the PIN entry system. The main aim of these methods was to provide complete security to the PIN entry. But, these methods did not provide the complete security. Some of such existing methods are discussed below.

Security-Improved Personalized Identification Number Entry Measures: Related Work: To deal with these non-technical attacks, one promising intervention is through the user interface (Matsumoto and Imai, 1991). The

main aspect has been incorporating indirect key entry measures to separate the visible keyed entry parts from the secret ones. Earlier research with passwords investigated cognitive authentication within the limitations of humans. Rothetal used two colors for indirect PIN entry in the method we call Binary PIN (Abdullah Ali, 2006). In each round, the system colored a random half of the numeric keys black and the other half white so users could enter the color of the PIN key by pressing a separate color key. Multiple rounds were played to enter a single digit of the PIN and repeated until all PIN digits were entered (Yoshihiro Kita, 2013).

Delayed Oracle Choices (DOC): If the oracle responds slowly then the partitions are exposed longer to the observer. When the exposure is longer, it is easier for the observer to manually record a partition. In the delayed oracle choices approach, n rounds are displayed consecutively with a predetermined exposure period of 0:5 seconds. The display is cleared subsequently and only then do the left and right input buttons appear. Using these buttons, the oracle must consecutively input the coloring that his PIN digit had in these n rounds. The oracle has only a limited period of time to determine the color of the current PIN digit in each round, and the color sequence must be memorized. This procedure is repeated until all PIN digits are entered.

2. PROPOSED METHOD

To address camera-based shoulder-surfing attacks over multiple authentication sessions and also to migrate users already familiar with the standard PIN entry system, this paper presents a novel PIN entry method called SteganoPIN. The SteganoPIN system builds on the concept of challenge-response rendered over a user interface and physical hand protection to advance the following goals for PIN-based authentication.

Usability: Must use the regular numeric keypad for key entry. Must incur limited increases in PIN entry time and error rates. Must not increase the length of a long-term PIN. Must stay within the short-term memory requirements of human limitations, such as four groups of items.

Strong Security: Must be resilient to camera-based shoulder-surfing attacks over multiple authentication sessions. Must resist active guessing attacks without allowing more advantage than random guessing.

The procedure can be repeated if the PIN length (i.e., the mapped OTP length) is greater than the limitation of the user's short-term memory or if the OTP is forgotten before entry. When the user revisits the challenge keypad explicitly, the system must refresh random challenges. Due to the random mapping between the two keypads, the system can verify the user's PIN from the OTP entry.

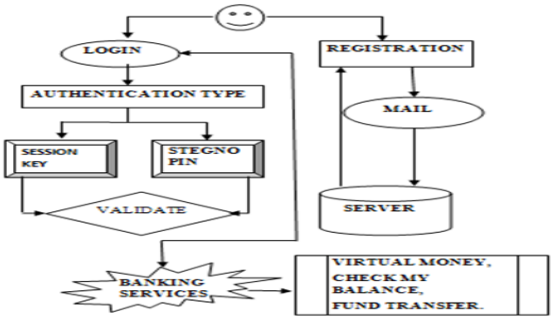

Figure.1. Architecture Diagram

Steganopin Security: In the two-faced keypad system, users familiarity with the regular key locations of the long-term PIN can ease the OTP derivation process, but as shown in Fig. 2 (d), an alternative de-sign of the challenge keypad incorporates regular indicators. Our Switch PIN was an early version of this method. We first designed SwitchPIN to secure PIN entry on a smartphone from human shoulder-surfers. In SwitchPIN, the user holds a show key to switch a regular layout keypad to a random permuted keypad for OTP derivation on the smartphone's touchscreen and then releases the show key to switch back to the regular key-pad for key entry. Switch PIN was vulnerable to camera-based shoulder-surfing attacks in only a single session and to a human shoulder-surfer over multiple sessions because the random key-pad just replaced the regular keypad in the same location. Thus, in this study, we separated the two keypads and reduced the size of the random challenge keypad. Overall, SteganoPIN satisfies

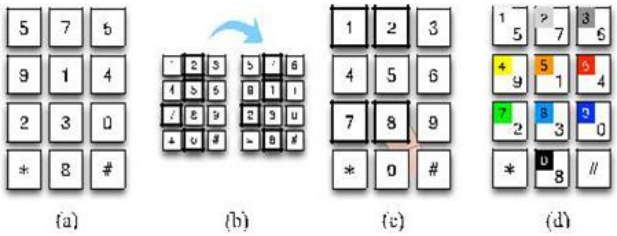

Figure.2. Two-faced keypad system.
(a) Challenge keypad, (b) OTP derivation process, (c) Response keypad, receiving the OTP input
(d) Alternative design of a challenge keypad

Prototype System: We implemented 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 key-pad), as in Fig.2(a). For OTP derivation, the user puts a cupped hand on the circle as in Fig.2(b) and reads the challenge keypad. For OTP entry, the user presses numeric keys on the response keypad as in Fig. 2(c). If the user forgets part of the OTP or the PIN length is greater than four digits, the user could repeat the procedure with another random challenge. Furthermore, hand use is flexible; for instance, a single hand for both OTP derivation and entry or both hands for OTP derivation work equally well. In practice, it is desirable to implement the circular touch area on both sides for right-handed and left-handed users.

The PIN space of SteganoPIN is 10^4 for a four-digit PIN chosen from the ten-digit alphabet set. With a guessing attack, the mth attempt of guessing, for $1 \leq m \leq 10^4$, because the challenge keypad and the response keypad render a one-to-one mapping in every authentication session. Thus, the Stegano PIN system can count the number of failed attempts and lock the account if it exceeds a small limit, as standard PIN systems do. To resist shoulder-surfing attacks, Stegano PIN uses a random challenge from a permuted keypad covered by a cupped hand. Adversaries could not derive a real PIN from the OTP without being able to see the challenge keypad. To investigate the security of the human–machine interactive protection of SteganoPIN, we simulated an OTP derivation process on an ATM simulation.

Session Key: In Session key Method, We propose improved tools to evaluate the resistance of PIN-entry method. First, we construct a theoretical framework to rigorously define and estimate the security. We then present experimental methods to support this framework. We also present an example PIN-entry method and show that this method is significantly more secure and usable than previous proposals. An improved tools to evaluate the resistance of a PIN-entry method.

Concept: Here the symbols replace the original pin. In the session key decision round, ten randomly arranged objects are displayed to the user. The user recognizes the symbol immediately below the first digit of his/her PIN as thetemporary session key and presses "OK." The user recognizes the symbol immediately below the first digit of his/her PIN as the temporary session key and presses "OK." Secured transmission of encrypted pin (one way).

Session keypad: The keypad of session key method is made up of two vertical array .one array contains numerals from 1 to 0 and another contains a set of special characters.These special characters are used in to denote the actual pin. For example, to enter the PIN is 2371, the user recognizes symbol as the session key because it is collocated with the first digit of the PIN, 2. The remaining rounds are PIN-entry rounds, in which the ith digit of the PIN is entered in the ith round for i= 2, 3, 4. In each of these rounds, the user is again given a random array of ten objects, and s/he enters a PIN digit by rotating the object array and aligning the session key with the current PIN digit. For this task, the user can use two additional buttons ("up" and "down"). In this example, the user presses the "down" button twice so that symbols moves to the position immediately below 3, and then presses "OK."

Session key Security: The security of this method is enhanced further. The shoulder surfing attackers can only know the pin in the form of symbols. Symbols replace the original pin. In the session key decision round, ten randomly arranged objects are displayed to the user. The user recognizes the symbol immediately below the first digit of his/her PIN as the temporary session key and presses "OK." The user recognizes the symbol immediately below the first digit of his/her PIN as the temporary session key and presses "OK.".

In the example shown where the PIN is 2371, the user recognizes symbol as the session key because it is collocated with the first digit of the PIN, 2. The remaining rounds are PIN-entry rounds, in which the ith digit of the PIN is entered in the ith round for i= 2, 3, 4. In each of these rounds, the user is again given a random array of ten objects, and s/he enters a PIN digit by rotating the object array and aligning the session key with the current PIN digit. For this task, the user can use two additional buttons ("up" and "down"). In this example, the user presses the "down" button twice so that symbols moves to the position immediately below 3, and then presses "OK." The decryption of the symbol is done at the bank side server to enhance its security to next stage by one way hashing.

User Registration: User Registration is done and only 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.

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 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 reduces the overhead complexities in the serverand will provide the User an ease of access to the Banking Services.

Algorithm:

Step 1: Registered users only shall be able to access the ATM application by their unique PIN in mobile phones.

Step 2: Enter the PIN which may be applied to any case with $N \geq 2$ digits. We need a total of four rounds.

- **Step. 1:** The first round is the session-key decision round, which is used for displaying ten randomly arranged objects to the user; the user then recognizes the symbol immediately below the first digit of his/her PIN as the temporary session key and presses "OK."
- **Step. 2:** Remaining rounds are PIN-entry rounds, in which the ith digit of the PIN is entered in the ith round for i = 2, 3, 4. In each of these rounds, the user is again provided with a random array of ten objects, and he/she enters a PIN digit by rotating the object array and aligning the session key with the current PIN digit.

Step 3: SteganoPIN simulates a horizontal ATM with a Smartphone and a tablet for OTP derivation.

Step 4: Once the user-entered pattern is manipulated and a PIN is identified, then the user can avail ATM services like cash withdrawal, deposit and fund transfer, which can be done securely using the concept of virtual money

3. EXPERIMENTAL RESULTS

User Registration is done and only 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. (Fig.3 & 4)

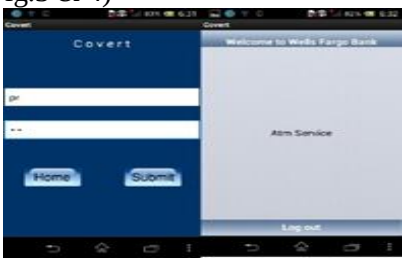

Figure.3. User Registration

Figure.4. Session Key

Figure.5. Structure Of Session Key (Password)

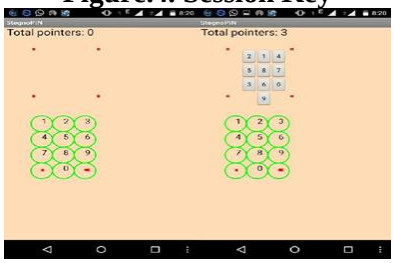

Figure.6. Stegano PIN

The User enters the login button and gives the user banking service will be opened. In the Stegano PIN Method they will select the appropriate password according the Structure. The PIN number that is entered by the user is verified by matching with the database in the server. When the PIN is sent through the public channel, there are some possibilities of hacking it. So, it is converted into the hash function and sent through the public channel.

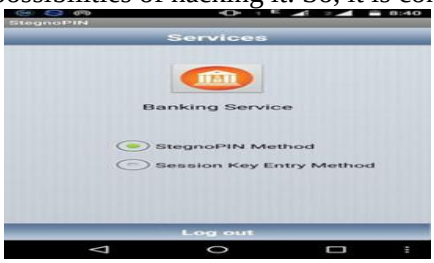

Figure.7. Banking page

When the PIN is verified the banking services will be opened for that particular user. The user can make the transactions such as PoS (Point of Sale), withdrawal, checking balance, mini statement, etc.

4. CONCLUSION

Therefore, the security in the PIN entry system of an ATM is enhanced using Stegano PIN and session key method by protecting it from various attacks. The concept of virtual money is used to show the banking services like fund transfer, check balance, withdrawal, deposit, etc.performed at the ATM terminal. For all these services a temporary password is generated to ensure security of the pin as the users reuse the same pin for various purposes. The fund transfer is also secured by the one way hashing of the pin done by using HMAC algorithm by protecting transmission during the public channel and also with generation of e-slip. In addition to this, the methods which are explained in the existing system (such as black white method and session key method) is also implemented in order to find a better statistics to show that the proposed method is the more secure and the safety method. The experimental results of the existing BW method and the proposed IBW method are shown in the form of graph. Specifically,

SteganoPIN has proven to be secure against camera-based shoulder-surfing attacks over multiple authentication sessions if a user properly used the system. SteganoPIN was also shown to be user-friendly based on its faster PIN entry time and lower error rates than other advanced-security PIN entry systems. The future work can extend this process for other bank-account transactions and to achieve further reduction in the time consumption

REFERENCES

Abdullah Ali, Ravi Kuber and Adam Aviv J, Developing and Evaluating a Gestural and Tactile Mobile Interface to Support Users Authentication, Conference, 2016.

De Luca A, Langheinrich M and Hussmann H, Towards understanding ATM security—A field study of real world ATM use, in Proc. ACM Symp, Usable Privacy Security, 2010, 1–10.

Greenberg A, Google glass snoopers can steal your pass-code with a glance, Wired, 2014.

Kwon T, Shin S and Na S, Covert attentional shoulder surfing, Human adversaries are more powerful than expected, IEEE Trans. Syst, Man, Cyber, Syst, 44 (6), 2014, 716–727.

Long J and Wiles J, No Tech Hacking, A Guide to Social Engineering Dumpster Diving and Shoulder Surfing, Boston, MA, USA, Syngress, 2008.

Matsumoto T and Imai H, Human identification through insecure channel, in Proc. Adv. Cryptal, 1991, 409–421.

Parti A and Qureshi F.Z, Integrating consumer smart cameras into camera networks, Opportunities and obstacles, IEEE Computer, May 2014 vol. 47 (5), 2014, 45–51.

Rogers J, Please enter your 4-digit PIN, Financial Services Technology, U.S. Edition, 4, 2007.

Roth V, Richter K and Feininger R, A PIN-entry method resilient against shoulder surfing, in Proc. ACM Computer Communication, Security, 2004, 236–245.

Song B, Ding C, Kamal A, Farrell J and Roy-Chowdhury A, Distributed camera networks, IEEE Signal Process, Mag, 28 (3), 2012.

Yan Q, Han J, Li Y and Deng R.H, On limitations of designing leakage-resilient password systems, Attacks, principles and usability, in Proc. 19th Internet Soc, Network. Distributed System Security Symp, 2012, 1–16.

Yoshihiro Kita, Fumio Sugai, MiRang Park, Naonobu Okazaki, Proposal and its Evaluation of a Shoulder-Surfing Attack Resistant Authentication Method, Secret Tap with Double Shift, International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2 (1), 2013, 48-55.