Steganopin:Two Faced Human-Machine Interface for Practical Enforcement of PIN Entry Security

Vani Viswanathan

Dept.of Computer Science, St.Joseph College (Autonomous), Irinjalakuda, Kerala, India

Abstract **-** steganopin two faced human machine interface for secure pin entry is the most secure way of pin entry.personalised identication number(PIN) is highly insecured due to various threats.to avoid this threats in banking transactions we introduced two practical way of pin entry with otp derivation ,they are stegano pin entry for fixed and limited transaction in online transaction as well as introducing a shuffled keypad using proximity sensor for deriation of otp for safer transaction.the two methods are mainly adopted for hiding the permanent of the user from any kind of shoulder surffing attacks using random generated numericals.user as the option to choose any one of the way of pin entry method throgh this application,once the pin number is entered the application is redirected towards users banking services.

Key Words: steganopin, steganopin authentication, shoulder surfing, security, personalised identification number, authentication

1. INTRODUCTION

A) Personalised Identification Number Entry Security Problems

Personal identification number(PINs)are widely used as a numerical password s for user authentication and various unlocking purposes.the pin entry applications are increasing day by day due to the development of touch screen makes a possible implementation of the pin entry on various commodities such as automated teller machine(ATM) ,point of scale POS terminals,debit cards etc.when we are directly entering a pin into ATM,security is easily compromised,particularly in public places and the nearby places the peoples can observe pin number by shoulder surfing by using automatic recording machines and manual tools like paper,pencil etc.thus a more secured way of transaction can be achieved in this proposed system.

The guessing attacker,shoulder surfing attacks and recording attacker is defined as a strong adversary having wearable cameras to record and analyze the entire transactions at a long range.the guessing attackers are those who tries to guess our pin number.they can also block the account by entering the wrong pin more than thrice.shoulder surfing is the direct observation technique of collecting the data.the vision enhancing tecniques helps the shoulder surfing attackers if the subjects are at far distance.in recording attack the attackers use the skimming devices and the miniature cameras to record and hack the pin.such attackers are becoming great threat now a days.

B) Security in personalised identification number entry measures

Inorder to deal with the non technical attackers an indirect way of entering have been introduced to separate the visible keyed entry parts from the secret ones.earlier research developed two types of keypad namely the response keypad and the challenge keypad.the response keypad is the keypad in which we enter our permanent pin wheras the challenge keypad is used for the derivation of the otp.the other method is the binary pin entry method in which two colors for indirect pin entry is used.each round the system is coloured a random half of the numeric key as black and other half white so the user needs to enter the colour by pressing separate color key.multiple rounds are played inorder to enter a single digit of the pin and are repeated till all pin digits are entered.

In the proposed system we are using two methods one is setting a virtual pin known as the steganopin for the fixed/limited transaction and the other method proposed is the steganopin authentication in which two types of keypads appears one with regular pattern and the other in shuffled form.tje users can make use of this shuffled keypad for deriving out their pin using an indirect entry.a proximity sensor is a sensor used in android phones which detects the presence of an object/person in vicinity of the devices sensor.proximity sensors are used in applications but are most widely used in smartphones.most of the modern android comes with IR based proximity sensor.

2. STEGANOPIN SYSTEM

This paper presents a novel pin entry method called steganopin.

The steganopin uses two types of keypad, response keypad and the challenge keypad. The response keypad appears with regular size infront of the user .the challenge keypad appears with a random layout for otp derivation.

The challenge keypad and response keypad advance the following goals for PIN- based authentication.

1) Usability: must use the regular numeric keypad for the key entry. Must not increase the length of the long term PIN

2) Strong security: it must be resilient to camera based shoulder surfing attacks.

A. Concept

The word stegano means concealed or protected .here the users generally derive out the otp instead of the permanent PIN.the numeric key entered by the user in plain view must be the one-time PIN(OTP) that conceals the real pin through instant derivation.inorder to make such derivation more convenient for the user there incorporate a two faced keypad system with two numeric keypads.also we are setting up a virtual pin for the secure banking transactions either as fixed or limited.

3. Two-faced keypad system

There are two types of keypad implemented in this system, one numeric keypad is a standard keypad in regular pattern and the other is the small separate keypad in random layout.the random keypad is known as the challenge keypad as it displays the numeric keys as a random challenge.the numeric keypad or the response keypad is used to enter our permanent PIN whereas the challenge keypad is used to derive out the OTP that is concealed in the real pin.

The user first locates the long term PIN in regular layout and subsequently maps the location of the key into the challenge keypad for OTP derivation.the user then enters this OTP on the regular keypad called the response keypad inorder to perform more safer transactions.this process is repeated if the PIN length is greater than the users short term memory.

In the shuffled keypad method the challenge keypad does not appear immediately,only the response keypad appears with the regular pattern and size.while we are covering the proximity sensor provided in our android phone,the challenge keypad appears with random numbers known as the shuffled numbers.

The challenge keypad disappears immediately after when the user releases his/her hand from that layout. Using this procedure, the human user and the machine system can interactively protect the challenge keypad from visually occluding it from the adverseries.thus enabling more security for the PIN entry and therefore establishes a safer transactions. The proximity sensor, available on new smart phones, could be used as an additional tool.

The other method proposed is the setting up of a virtual PIN called the steganopin for the safer online secure transaction.here in this method; a virtual pin is set by the card holder and is given for the third party given a fixed /limited permission of transaction.

In this method also an OTP is generated into the registered phone number and after that a virtual PIN is set either for fixed/limited transaction.it is considered to be the more secure way of online transaction.

SteganoPIN security

- The PIN space of the steganopin is the four-digit PIN choosen from the ten digit alphabet set.
- To resist the shoulder surfing, guessing, recording attacks, steganopin uses the random challenge from the permutedkeypad.
- Adversaries could not derive a real PIN from the OTP without being able to see the challenge keypad.
- As we are setting up a virtual pin for both the fixed/limited transaction most of the shoulder surfing attacks,guessing attacks can be considered to be ineffective.

Overall, steganopin satisfies strong security goals.that,is steganopin is resilient to camera-based shoulder surfing attacks over multiple authentication sessions if the system is properly installed and used.it is secure against active guessing attacks,recording attacks,and the shoulder surfing attacks.

Once the user have entered the OTP their respective pin number is iden tified. The pin number will be checked with the loca l database provided by the Sol. lite in order to contin ue the transaction, then one way hash method has been generated for the validation of pin entry that has been send to the server in the public channel so that the attacker cannot guess the pin by monitoring the channel .After verification the mobile app will provide a response to redirect the user to the services. In ATM services cash withdrawal and deposit and fu nd transfer can be done safely.

Advantages

1) Transaction of money is safer: the two methods provides a more safer way of transaction using two different methods of the PINentry.

2) Security of the PIN also achieved: the direct entry of our pin can be avoided in this methods described.the pin number is more secure.

3) limited/fixed way of transaction: we can limit or fix our transaction using this method.

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) For OTP derivation.
- the user puts a handonthecircleasiandreads thechallengekeypad. For OTP entry, the user presses numeric keys on the response keypad .
- 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 equallywell.Inpractice,
- It is desirabletoimplementthecircular touch area on both sides for right-handed and left-handed users.

- The PIN space of SteganoPIN is 104 for a four-digit PIN chosen from the ten-digit alphabet set.

- With a guessing attack, the success probability is m 104 for m attempts and 1 104−m+1 forthe mth attempt of guessing, for 1≤ m ≤104, because the challenge keypad and the response keypad render a one-to-one mapping in every authentication session.

- The SteganoPIN system can count the number of failure attempts and lock the account if it exceeds a small limit, as standard PIN systems do.

users could without difficulty authenticate themselves to the SteganoPIN system by generating an OTP on the basis of a long-term PIN.

SteganoPIN would be slower than the standard system in PIN entry time.

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 keypad).

hand use is flexible; for instance, a single hand for both OTP derivation and entry , both hands for OTP derivation.

To make such a derivation process secure against adversaries, we incorporate a human–machine interactive protection method 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.

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.

BANKING AND SERVICES

- Once the user has e ntered the OTP their respective pin number is iden tified.
- The pin number will be checked with the loca l database provided So in order to contin ue the transaction, then one way hash method has been generated for the validation of pin entry which has been send to the server in the public channel so that the attacker cannot guess the pin by monitoring the channel .
- After verification the mobile app will provide a response to redirect the user to the services.
- In ATM services cash withdrawal and deposit and fu nd transfer can be done safely.
- **Authentication**
- In the context of computer systems, authentication is a process that ensures and confirms a user's identity.
- Authentication is one of the five pillars of information assurance (IA). The other four are

integrity, availability, confidentiality and nonrepudiation.

- Once the user have login to the mobile application using his account number and the unique PIN number. The next step is the authentication.
- While setting up the virtual pin, an OTP is sent to the registered phone number, at that particular time the card holder can either fix/limit the transaction amount to the third party.
  - Authentication begins when a user tries to access information.
  - First, the user must prove his access rights and identity. When logging into a computer, users commonly enter usernames and passwords for authentication purposes. This login combination, which must be assigned to each user, authenticates access.
  - However, this type of authentication can be circumvented by hackers.
  - Athentication is considered to be important because it enables the organisation to keep network secure.

Conclusion

Our paper is proposed to mi nimize the attacks that prevail in ATM transactions. This mobile application will be more useful to this digital world which lacks in security. This is simple to install. Hence leads to the safer transactions of money between the bank and the customer.

REFERENCES

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

2) A. Greenberg. (2014, Jun.). Google glass snoopers can steal your passcode with a glance," Wired. [Online]. Available: http://www.wired.com/ 2014/06/google-glass-snoopers-can-steal-your-passcode-with-a-glance/

3) V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient againstshouldersurfing,"inProc.ACMComput.Commun.Security,2004, pp. 236–245.

4) T.Kwon,S.Shin,andS.Na,"Covertattentionalshouldersurfing:Human adversaries are more powerful than expected," IEEE Trans. Syst., Man, Cybern., Syst., vol. 44, no. 6, pp. 716–727, Jun. 2014.

5) 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.

6) A. Parti and F. Z. Qureshi, "Integrating consumer smart cameras into camera networks: Opportunities and obstacles," IEEE Comput., vol. 47, no. 5, pp. 45–51, y 2014.

7) B. Song, C. Ding, A. Kamal, J. Farrell, and A. Roy-chowdhury, "Distributed camera networks," IEEE Signal Process. Mag., vol. 28, no. 3, pp. 20–31, Apr. 2011.

8) A.DeLuca,M.Langheinrich,andH.Hussmann,"Towards understanding ATMsecurity—AfieldstudyofrealworldATMuse,"inProc.ACMSymp. Usable Privacy Security, 2010, pp. 1–10.

9) J.Rogers,"Pleaseenteryour4-digitPIN,"FinancialServicesTechnology, U.S. Edition, vol. no. 4, Mar. 2007.

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

11) S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in Proc. ACM Int. Working Conf. Adv. Visual Interfaces, 2006, pp. 177–184.

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

13) A.DeLuca,K.Hertzschuch,andH.Hussmann,"ColorPIN–SecuringPIN entry through indirect input," in Proc. ACM

14) 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.

15) P. Golle and D. Wagner, "Cryptanalysis of a cognitive authentication scheme," in Proc. IEEE Symp. Security Privacy., 2007, pp. 66–70.

16) T. Kwon and J. Hong, "Analysis and improvement of a PIN entry method resilient to shoulder-surfing and recording attacks," IEEE Trans. Inf. Forensics Security, vol. 10, no. 2, pp. 278–292, Feb. 2015.

17) H. Sasamoto, N. Christin, and E. Hayashi, "Undercover: authentication usable in front of

prying eyes," in Proc. ACM SIGCHI conf. Human Factors Comput. Syst., 2008, pp. 183–192.

18) 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.

19) 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.

20) 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.

21) A. Bianchi, I. Oakley, and D. S. Kwon, "Counting clicks and beeps: Exploringnumerositybasedhapticandaudiopinentry," InteractingComput., vol. 24, pp. 409–422, 2012.

22) T. Perkovic, A. Mumtaz, Y. Javed, S. Li, S. A. Khayam, and M. Cagalj, "Breaking undercover: Exploiting design flaws and nonuniform human behavior,"