ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Improvement of Pin-Entry Method Using Hybrid Images and OTP

B.Hema, Prathibha.P, Sharmila.N. Umadevi.A.

Department of Information Technology, Velammal Institute of Technology, Chennai, Tamil Nadu, India

ABSTRACT: In current ATM process there is lot of ATM fraud Malicious money transaction and theft are happens by means of lack of privacy protection in current scheme. We address the problem of shoulder-surfing attacks on authentication schemes by proposing Illusion PIN (IPIN), a PIN-based authentication method that operates on touch screen devices. IPIN uses the technique of hybrid images to blend two keypads with different digit orderings in such a way, that the user who is close to the device is seeing one keypad to enter her PIN, while the attacker who is looking at the device from a bigger distance is seeing only the other keypad. The user's keypad is shuffled in every authentication attempt since the attacker may memorize the spatial arrangement of the pressed digits. To reason about the security of Illusion PIN, we developed an algorithm which is based on human visual perception and estimates the minimum distance from which an observer is unable to interpret the keypad of the user. In addition, we estimated the minimum distance from which a camera is unable to capture the visual information from the keypad of the user. Based on our analysis, it seems practically almost impossible for a surveillance camera to capture the PIN of a Smartphone user when IPIN is in use. In current scheme we also implement the OTP authentication mechanism. This will enhance more security which is attached with virtual Keyboard of ATM machine. So we proposed the concept of ATM protection including shuffling keyboard with OTP authentication.

KEYWORDS: PIN Authentication, Shoulder -Surfing, Video Attack, Hybrid Image, Human Visual Perception

I. INTRODUCTION

User authentication is performed in various ways. Wefocus on PIN authentication because of its simplicity and maturity. A Personal Identification Number (PIN) is a sequence of digits that confirms the identity of a person when it is successfully presented. PINs are simpler than alphanumeric passwords as they solely consist of numerical characters (0-9) and have a short length that is usually either 4 or 6 digits.This makes PINs easy to remember and easy to reproduce, and as a consequence, PIN authentication is characterized by infrequent errors. So, simplicity is translated to usability. The maturity of PIN authentication is a result of its continuoususage for years in a wide range of everyday life applications,like mobile phones and banking systems.

II. PROBLEM DEFINITION

We address the problem of shoulder-surfing attacks on authentication schemes by proposing Illusion PIN (IPIN), a PIN-based authentication method that operates on touch screen devices. IPIN uses the technique of hybrid images to blend two keypads with different digit orderings in such a way, that the user who is close to the device is seeing one keypad to enter her PIN, while the attacker who is looking at the device from a bigger distance is seeing only the other keypad. The user's keypad is shuffled in every authentication attempt since the attacker may memorize the spatial arrangement of the pressed digits.

III. PROPOSED SYSTEM

Illusion PIN (IPIN) for touch screen devices. The virtual keypad of IPIN is composed of two keypads with different digit orderings. **The Visibility Algorithm** is can be used to assess the visibility of images. **Shuffling**

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Algorithm is used for shuffle the keypad. The user's keypad is shuffled in every authentication attempt. **Random Generation Algorithm** is used to generate one time password (OTP)
Illusion PIN-based authentication scheme would be resistant against shoulder surfing attacks. The user's keypad is shuffled in every authentication attempt. In public place we don't need to use our PIN number, in that time OTP is helpful for our Money transaction. PINs are short and require just a small numeric keypad instead of the usual alphanumeric keyboard. In addition, PIN authentication is often performed in crowded places, e.g.,

when someone is unlocking her mobile phone on the street or in the subway. Shoulder-surfing is facilitated in such scenarios since it is easier for an attacker to stand close to the user while escaping her attention.We designed Illusion PIN (IPIN) for touch screen devices. The virtual keypad of IPIN is composed of two keypads with different digit orderings, blended in a single hybrid image. The user who is close to the screen is able to see and use one keypad,

but a potential attacker who is looking at the screen from a bigger distance, is able to see only the other keypad. We developed an algorithm to estimate whether or not the user's keypad is visible to an observer at a given viewing position. We tested the estimated visibility of Illusion PIN through a user study of simulated shoulder-surfing attacks on Smartphone devices. We estimated the minimum distance from which a camera is unable to capture the visual information from the user's keypad. The results show that it is practically almost impossible for a surveillance camera to capture the PIN of a Smartphone user when Illusion PIN is in use. Random generation algorithm is used to generate one time password (OTP) which is send to our email or phone number, we can use this OTP for amount transaction in ATM, petrol bank, shopping mall and so on in public place. This technique will enhance the protection mechanism while withdrawal of money from ATM and other process.

IV. IMPLEMENTATION

- Holder account application Module
- Hybrid Image Module
- OTP Generation Module
- Virtual keyboard Module
- ATM transaction Module

Holder account application Module:

In this module the holder is going to create an account with some bank mandatory field, these fields are used in further upcoming process. This module is like a privilege form to get an action in bank service.

Hybrid Image Module:

We are using Visibility Algorithm to create Hybrid Images. Hybrid Images are images, The visibility algorithm analyzed the visual capacity of human eyes and generate mild images that can able to see in a particular nearby distance, but cant seen long distance.

OTP Generation Module:

One Time Password is generated by using Random Generation Algorithm which is sent to account holder's mail when the card is going to be swiped. This will enhance the additional security level in ATM transaction.

Virtual keyboard Module:

We create the alternate solution for security in ATM PIN ENTRY Method by generation of virtual keyboard. In this key board we implement random keys using Shuffling algorithm at the transaction of every time.

ATM transaction Module:

In this module get the input like an pin number through the ATM keypad, Actually our Application Provide the keypad number are changing in dynamically so the hacker cant able to hack the pin Number.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

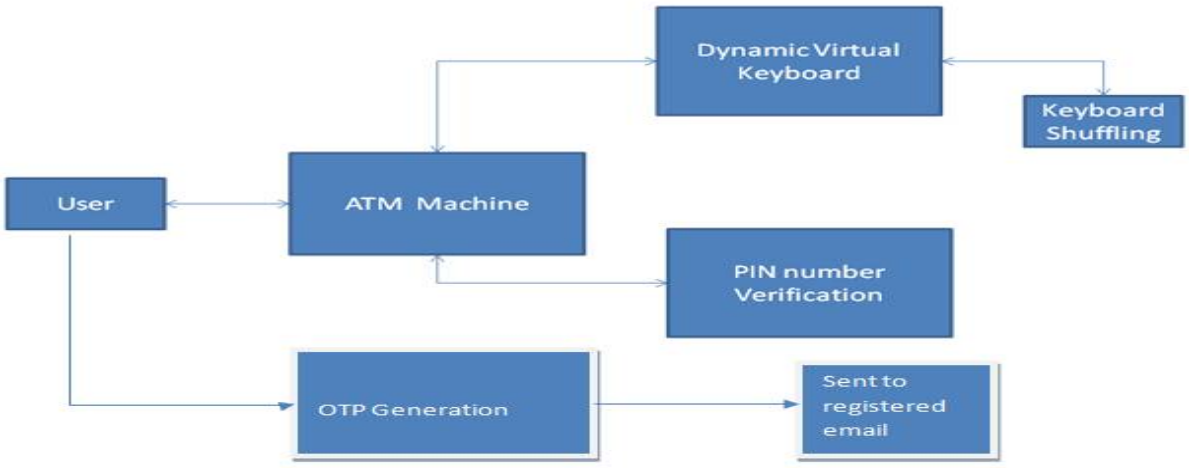
International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

SYSTEM DESIGN



V. ALGORITHMS USED

VISIBILITY ALGORITHM

The visibility algorithm receives as inputs a hybrid keypad *I* and a viewing position *N* in the 3D space. It returns a binary prediction on whether the user's keypad of *I* is visible to an observer who is in position *N*. We use this prediction either to estimate the minimum safety distance that corresponds to a given hybrid keypad, or to create a hybrid keypad that respects a given safety distance. Algorithm 1 provides the pseudo code of the visibility algorithm.

Visibility Index: In the second step of our algorithm, we compute the visibility index which quantifies how visible the user's keypad of *I* from the viewing position *N* is. Threshold Value of the Visibility Index: Let's assume that we are given a hybrid keypad I and an observer who first views *I* from position *N*1 and then from position *N*2. If the corresponding visibility index values are *v*1 and *v*2 and holds *v*2 > *v*1, we expect the user's keypad to be less visible from position *N*2 than from *N*1. If *v*1 ' *v*2, we expect the user's keypad to be almost equally visible in both cases. This is a direct consequence of the way we have defined the visibility index. Now let's assume that two different hybrid keypads *I*1 and *I*2 are viewed by the same observer from positions *N*1 and *N*2, respectively. If the corresponding visibility index values are *v*1 and *v*2 and holds *v*2 > *v*1, we expect the user's keypads of *I*1 to be more clearly visible than that of *I*2. Similarly, if *v*1 ' *v*2, we expect the user's keypads of *I*1 and *I*2 to be almost equally. This is the main assumption that we make about the behavior of the visibility index and we expect to hold in its reverse form too. This means that if the user's keypad from a hybrid keypad *I*1 is more clearly visible than the user's keypad of a different hybrid keypad *I*2 when they are viewed from positions *N*1 and *N*2, respectively, then for the corresponding visibility index values *v*1 and *v*2 we expect to hold *v*2 > *v*1.

VI. ADVANTAGES

- The main goal of our work was to design a PIN-based authentication scheme that would be resistant against shoulder surfing attacks. To this end, we created Illusion PIN.
- We quantified the level of resistance against shoulder-surfing by introducing the notion of safety distance, which we estimated with a visibility algorithm. In the context of the visibility algorithm, we had to model at a basic level how the human visual system works.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

- The user's keypad is shuffled in every authentication attempt since the attacker may memorize the spatial arrangement of the pressed digits.

VII. CONCLUSION

The main goal of our work was to design a PIN-based authentication scheme that would be resistant against shoulder surfing attacks. To this end, we created Illusion PIN. We quantified the level of resistance against shoulder-surfing by introducing the notion of safety distance, which we estimated with a visibility algorithm. In the context of the visibility algorithm, we had to model at a basic level how the human visual system works. In this process, we made a number of simplifying assumptions that limit the accuracy of our calculations. Our future work could conclude that the visibility algorithm could be used to assess the visibility of general images, but its parameters have to be appropriately tuned for the particular task at hand.

REFERENCES

[1] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012, pp. 553–567.
[2] M. Harbach, A. De Luca, and S. Egelman, "The anatomy of smartphone unlocking," in Proceedings of the 34th Annual ACM Conference on Human Factors in Computing Systems, CHI, 2016.
[3] J. Bonneau, S. Preibusch, and R. Anderson, "A birthday present every eleven wallets? the security of customer-chosen banking pins," in Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2012, vol. 7397, pp. 25–40.
[4] R. Anderson, "Why cryptosystems fail," in Proceedings of the 1st ACM Conference on Computer and Communications Security. ACM, 1993, pp. 215–227.
[5] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens." WOOT, vol. 10, pp. 1–7, 2010.
[6] A. Oliva, A. Torralba, and P. G. Schyns, "Hybrid images," ACM Transactions on Graphics (TOG), vol. 25, no. 3, pp. 527–532, 2006.
[7] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. W. Nicholson, J. Nicholson, and P. Olivier, "Multi-touch authentication on tabletops," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2010, pp. 1093–1102.
[8] L.-W. Chan, T.-T. Hu, J.-Y. Lin, Y.-P. Hung, and J. Hsu, "On top of tabletop: A virtual touch panel display," in Horizontal Interactive Human Computer Systems, 2008.
TABLETOP 2008. 3rd IEEE International Workshop on. IEEE, 2008, pp. 169–176.
[9] W. Matusik, C. Forlines, and H. Pfister, "Multiview user interfaces with an automultiscopic display," in Proceedings of the working conference on Advanced visual interfaces. ACM, 2008, pp. 363–366.