International Journal of Trend in Scientific Research and Development (IJTSRD)

International Open Access Journal

ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

ATM Security System by using Hybrid Authentication

V. Saravanan, M. Sathishkumar, M. Babu
Department of Computer Science Engineering,
G.K.M College of Engineering and 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: *shuffling keyboard, pin generation, one time password (otp)*

INTRODUCTION

In this paper we discuss about 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. Shoulder-surfing refers to eavesdropping personal information, like an alphanumeric password or a PIN, through observation. A typical example is an adversary who is standing behind a person in the line for an ATM machine and is looking, or "surfing", over the person's shoulder to obtain her PIN information. In this scenario, the attacker is observing a person while being in her vicinity. However, the attacker may observe someone remotely by using recorded material that was collected intentionally or even unintentionally. shoulder-surfing material could result from a surveillance camera that captured a person while entering her authentication credentials to unlock her phone in a store or at the workplace. Authentication schemes which are not resilient to observation are vulnerable to shoulder surfing. Any kind of visual information may be observed, including the blink of a button when it is pressed, or even the oily residue that the fingers leave on a touch screen. Shoulder-surfing is a big threat for PIN authentication in particular, because it is relatively easy for an observer to follow the PIN authentication process. 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.

RELATED WORK

Shoulder surfing resist authentication schemes by using design principles. The principle states that visual information has to cover user keypad by Cupping one hand while using the other hand to enter the pin. The alternative solution that does not require extra effort from the user is to make the content of the screen visible within a limited range of viewing distance. The visual complexity principle states that it has to be difficult to receive visual information and hybrid images that allow the user to secure password for touch screen and keypad. if the attacker is able to observe multiple times during the authentication process or to record it, he may to able steal the credentials of the user. The cognitive complexity principle states that it has no be difficult to process the acquired visual information. The user is required to enter her pin in the following way.

The digits on the provided keypad are separated into two sets based on their color. Half of them are black, and half of them are white. The user selects the set that the current digit belongs to, and then the digit are reassigned to the two colour sets. This procedure is repeated until the scheme is able to uniquely determine the correct digit by intersecting the selected sets. The user proceeds to the next digit of her pin. For an observer its difficult to successfully perform sequential inetrsections of sets to extract the correct pin. The alteration principle states that the required input has to change in every authentication attempt. In each authentication attempt, different images from the portfolio are assigned to the set of images.

PROPOSED SYSTEM

We used 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.

Architecture diagram

User

ATM Machine

Dynamic Virtual Keyboard

Keyboard Shuffling

PIN number Verification

MODULE:

- ATM card and account formulation module
- Account holder info updating module
- ATM transaction by shuffling key pad module
- View holder last little transaction
- OTP Generation module

MODULE DESCRIPTION

ATM CARD AND ACCOUNT FORMULATION MODULE

In this module is used to do formalities to get an ATM card like an ATM card Request. The holder's Account Number and pin number are sending to our E-mail, through the save our time because now a days the account holders are wasting the time to complete their initial process.

ACCOUNT HOLDER INFO UPDATING MODULE

In this module Update the users detail when he need, the ATM card are supposed to lose in that time the going to give new ATM card Request and we update the Pin detail in that particular Holders.

ATM TRANSACTION BY SHUFFLING KEY PAD 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.

VIEW HOLDER LAST LITTLE TRANSACTION

In this module is used to provide the last few transactions are made in those particular domain users. This transaction detail consist of transaction amount,

Area of ATM, Transaction Time and Date Details.

OTP GENERATION MODULE:

In this module, OTP is generated and sent to the registered emailId of the user.

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. The most obvious example is the pinhole camera model that we used to describe the image formation process in the eye. The visibility algorithm forms the core of our work and we would like to examine whether it can be used to assess the visibility of images other than hybrid keypads. The visibility algorithm uses the MSSIM index which quantifies the distortion between two images.

REFERENCES

1. D.K.YADAV,B.IONASCU,S.V.K.ONGOLE "Design and analysis of shoulder surfing resistant pin authentication mechanism google glass"
2. R.Dhamija and A.Peerig."using the image for authintication based on graphical password
3. Z.Li,Q.Sun,Y.lin an association based grapical passwod design resistant to shoulder surfing attack"
4. T.perkovic and N.Saxena "shoulder surfing safe logging in paritally observable attacker model"
5. A.De.luca and H.Hussmann" securing pin entering through indirect pin"