www.ijiarec.com

ISSN:2348-2079

Volume-7 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Pin Security Scheme Using Haptic Feedback

Mr.S. Karuppusamy[1], Monalisa Koley[2], N.Nagapavithra[3], V.Shanthidevi[4], P.P.Shobana[5]

[1]Associate Professor, Department of computer science and engineering, Nandha Engineering College (Autonomous)

[2-5]UG students, Department of computer science and engineering, Nandha Engineering College (Autonomous)

ABSTRACT

The common pin-entry schemes are vulnerable to observation attacks. In order to enhance the resistance to observation attacks, the pin-entry schemes for mobile devices based on audios and haptics are planned. However, none of existing observation attacks resistant cannot provide good security and usability compared to the new observation attacks. The pin-entry schemes can achieve both security and high usability. Herein, we have a tendency to propose a new observation attacks resistant pin-entry scheme, Loc-happin for touchscreen devices providing localized haptic feedback. By victimization the technology of localized haptic feedback, the usability and the resistance to observation attacks are improved. Furthermore, the user can choose the efficiency-security setting suitable for him.

Keywords: shoulder surfing attacks, user authentication, pin identity theft

INTRODUCTION

In existence without the proper usage of security or locks in Mobile Phones which leads to vulnerability of stealing others personal information. This personal information involves misusing others photo's, banking details, getting some important documents being misused by others without proper security scheme. The problem of security is growing very bad due to smart phone usage.

This project is a mobile application based project to enhance security. It is a user-friendly software application. The purpose of this project is to provide a better security, a software solution that delivers a scalable, secure, and reliable application that maintains and manages the application details. Personal Identification Number (PIN) is a numeric password that can be used for user authentication. As common PIN- entry schemes are vulnerable to observation attacks, in which the adversary can obtain the user's PIN by using should surfing attacks or camera recording attacks, Roth et al.

Proposed an observation attacks resistant PIN-entry scheme, IOC. However, the resistance of IOC to observation attacks is insufficient. Since then, many observation attacks resistant PIN-entry schemes have been proposed. However, the Resistances of these schemes to observation attacks or accidental login are unsatisfactory. To enhance the resistance to observation attacks, some observation attacks resistant PIN- Entry schemes supported audios or haptics are projected. However, none of those schemes are able to do each smart security and high usability.

Conventional touchscreen devices offer no localization of the haptic feedback. Recently, touchscreen devices providing localized haptic feedback have been designed. It seems that touchscreen devices providing localized haptic feedback will be available for users in the near future. We find that the feature of localized haptic

Author for correspondence:
Department of computer science and engineering, Nandha Engineering college (Autonomous)

feedback can be used to enhance the usability of observation attacks resistant PIN-entry schemes. Herein, we will propose an efficient observation attacks resistant PIN-entry scheme, Loc-HapPIN, using localized haptic feedback. We will show that Loc-HapPIN can achieve both good security and high usability.

RELATED WORKS

In the past decades, tons of analysis on word authentication has been tired the literature. Among all of those planned schemes, this paper focuses principally on the graphical-based authentication systems. Roth et al. [1], in 2004, planned Associate in Nursing observation attacks resistant PIN-entry theme, IOC (Immediate Oracle Choice). The login screen of IOC may be a regular PIN pad. 1/2 the numbers on the regular PIN pad square measure in black background and therefore the remaining numbers on the regular PIN pad square measure in white background. The user must acknowledge the background color of his PIN digits by clicking either the black button or the white button. Because the user must end four stages for one digit, a 4-digit PIN needs sixteen stages. On the opposite hand, because somebody will simply compare the determined login stages to eliminate most false PINs, the resistance of IOC to observation attacks is weak.In 2009, Shi et al. [4], proposed a rotary observation attacks resistant 4-digit PIN-entry scheme with two variants, VO and VT. However, as the success probability of observation attacks of VO is only 10 1, the resistance of VO to observation attacks is weak. On the other hand, as the success probability of accidental login of VT is only 10 2, the resistance of VT to accidental login is weak. Later, Lee [2], in 2014, proposed two observation attacks resistant 4-digit PIN-entry schemes, LIN4 and LIN5. However, the resistances of LIN4 and LIN5 to observation attacks are weak.

To enhance the resistance to observation attacks, haptics have been used. In 2011, Bianchi et al. [6] proposed an observation attacks resistant 4-digit PIN-entry scheme, the haptic version of Phone Lock, which uses haptics as the secondary channel on mobile devices. Unfortunately, its average login time is long. Furthermore, its resistance to accidental login is weak. In 2012, Bianchi et al. [7] proposed a haptics based observation attacks resistant 4-digit PIN-entry scheme, Time Lock. However, the resistance of Time Lock to observation attacks is weak. Later, Kuribara et al. [8] proposed a haptics based observation attacks resistant 4-digit PIN-entry scheme, VibraInput. However, its usability is not ideal.

In 2010, David Kim et al. planned a visible authentication theme for work surface interfaces referred to as ”Color Rings”, wherever the user is allotted i authentication (key) icons, that square measure together allotted one in all the four color-rings: red, green, blue, or pink. Throughout login, I grids of icons square measure provided, with seventy two icons being displayed per grid. There's just one key icon conferred in every grid.

The user should drag all four rings (ideally with finger and thumb from 2 hands) at the same time and place them within the grid. The distinct key icon ought to be captured by the right color ring whereas the remainder of rings simply create decoy picks. The user confirms a variety by dropping the rings in position.

In order to defend the shoulder surfing attacks with video capturing, FakePointer was introduced in 2008 by T. Takada. In addition to the PIN number, the user will get a new “answer indicator” each time for the authentication process at a bank ATM. In other words, the user has two secrets for authentication: a PIN as a fixed secret and an answer indicator as a disposable secret. The answer indicator is a sequence of n shapes if the PIN has n digits. This approach is quite robust even when the attacker captures the whole authentication process.

PROBLEMSTATEMENT, ATTACK MODEL

Problem statement

With the increasing quantity of mobile devices internet services, users will access their personal accounts to send confidential business emails, transfer photos to albums within the cloud or remit cash from their e-bank account anytime and anyplace. Whereas work into services publicly,

they'll expose their passwords to unknown parties unconsciously.

Individuals with malicious intent might watch the entire authentication procedure through present video cameras and police work instrumentality, or maybe a mirrored image on a window. Once the aggressor obtains the countersign, they may access personal accounts which would positively create an excellent threat to one's assets. Shoulder surfboarding attacks have gained a lot of and a lot of attention within the past decade. The following lists the analysis issues we might prefer to address during this study:

- The downside of a way to perform authentication publically in order that shoulder surf riding attacks are often alleviated.
- The downside of a way to increase secret area than that of the standard PIN.
- The downside of a way to expeditiously search precise pass-word objects throughout the authentication section.
- The downside of requiring users to learn additional info or to perform additional computation throughout authentication.
- The downside of restricted usability of authentication schemes which will be applied to some devices solely.

ATTACK MODEL

Shoulder Surfing Attacks

Based on previous analysis users' actions lie writing from their keyboard, or clicking on the pass-images or pass-points publicly could reveal their passwords to folks with unhealthy intention. During this paper, supported the suggests that the attackers use, we have a tendency to reason shoulder-surfing attacks into 3 sorts as below:

- Type-I: Naked eyes.
- Type-II: Video captures the whole authentication method one time.
- Type-III: Video captures the whole authentication method quite once.

The latter kinds of attacks need a lot of effort and techniques from attackers. Thus, if an authentication theme is in a position to resist against these attacks, it's conjointly secure against previous kinds of attacks. A number of the planned authentication schemes together with ancient text-password and PIN, square measure prone to shoulder surf riding Type-I attacks and therefore are subject to Type-II and Type-III attacks.

These schemes reveal passwords to attackers as shortly as users enter their passwords by directly pressing or clicking specific things on the screen. Alternative schemes like those in will resist against Type-I however square measure prone to Type-II and Type-III attacks since the attackers will crack passwords by across their video captures from multiple steps of the whole authentication method.

Smudge attack

A smudge attack is associate implicit attack where attackers plan to extract sensitive information from recent users' input by inspecting smudges left on bit screens. In line with a previous study, authentication schemes that need users to the touch or fling on laptop monitors or show screens throughout the login part area unit liable to smudge attacks.

The aggressor will acquire the user's countersign simply by perceptive the smudge left on the bit screen. Since every the horizontal and vertical bars in unit of measurement scroll table, shifting on any half within the bar can flow into the entire bar.

Thus, users do not visit shift the bars by touching the login indicators. The smudge left by users is additionally quite mounted, but it alone indicates the habitual stretching vary of the thumb or finger.

The length of the smudge left on the screen to boot provides no useful information since the login indicator is generated pin and additionally the permutations of elements on every bars are each that approach re- arranged in every digit of pin and in each login session.

PROPOSED SCHEME — LOC-HAPPIN

In this section, we will describe a simple observation attacks (OA) resistant 4-digit PIN-entry scheme, Loc-HapPIN, for mobile devices based on localized haptic feedback. The main idea behind this application is to enhance the security.

Initially the user register the required fields and get the OTP.

The Random vibration for the each pin is generated. If someone try to misuse the pin their image is been capture and sent to the owner's registered mobile number. To enhance resistance to observation attacks, the proposed system uses a haptic feedback system with pure random generator using HRNG algorithm. Loc-HapPIN involves two phases, the registration phase and the login phase, which can be described below.

Registration Phase

Initially, a secure channel is established between the user and the system. The user need to register the required details to know that the required person use the mobile Username, mail id and the recovery phone number is set first and stored in the Database after the completion of first page, The second page with further details get displayed by clicking next.

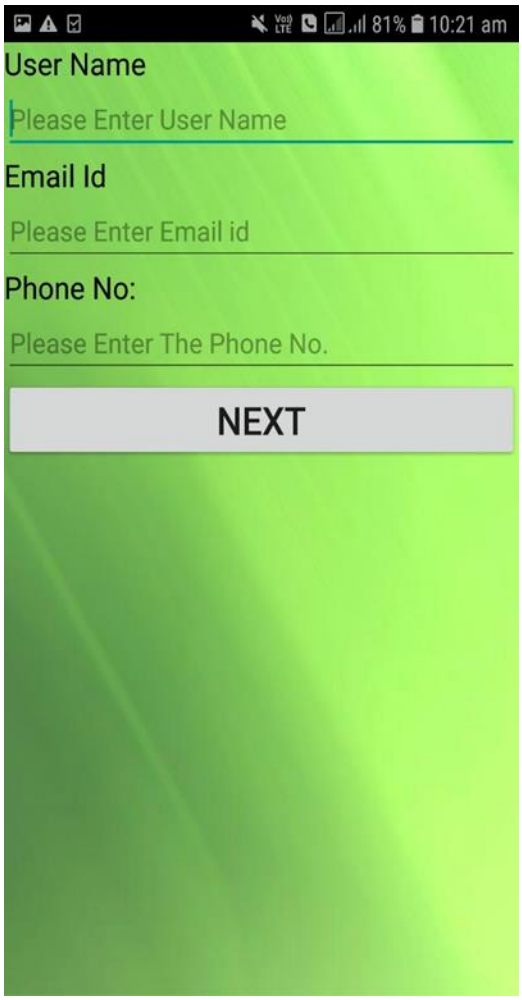

Fig. 1. The registration screen.

Login Phase

An OTP is shipped to the registered range when submitting the primary page. Enter the OTP, if you enter any range you will may get an error message that your OTP is wrong.

You're able to enter the positive identification the limit of the positive identification is restricted solely to 4digit, the protection question are often entered by the user and also the security answer is additionally set by the user, it keep within the info by clicking next.

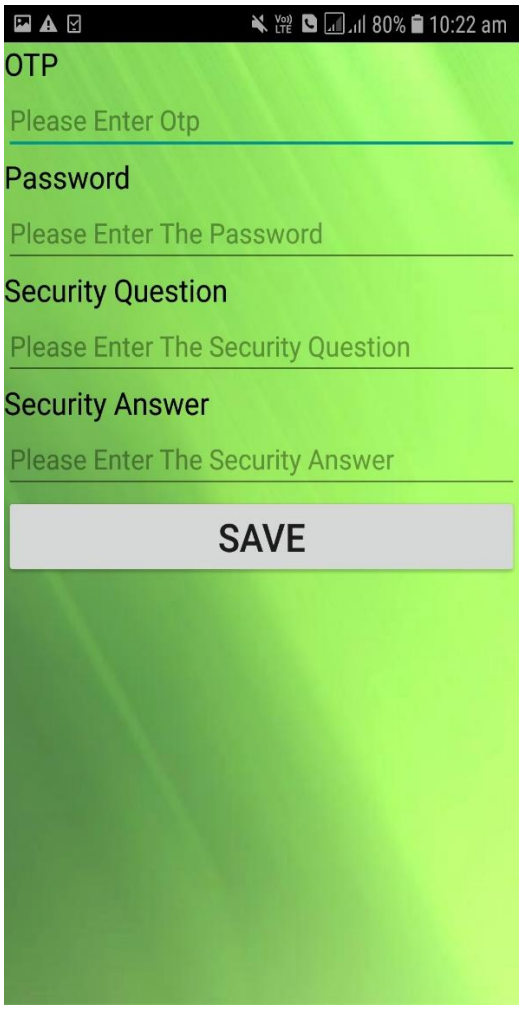

Fig. 2. OTP confirmation screen

To log into the system, the user has to finish the following steps: Step 1: The user requests to log into the system. A secure channel is established between the user and the system.

Step 2: The system displays the login screen according to the selected efficiency-security setting. The user has to hold the device for the haptic sensation region of the screen of the challenge state. Next, only one of the five contact points will be randomly chosen to induce a random vibration pattern. The user can sense the vibration pattern (hint), remember the pass- digit, which is indicated by the hint.

Step 3: For the password for each pin we get vibration between (1-5) times. Enter the pin after the vibration stops then the vibration starts for the second pin this step repeats for each registered pin. After the pin is entered. Press entered. If the password and the vibration matches if the pin that we have entered is right then we go to the next module the app which is secured will display. The user has to find the target slot and the i-th digit of PIN in the digits-pad. Let i = i + 1. According to the selected efficiency-security setting, the operations specified in the corresponding case are executed. If the user has correctly dragged all his PIN digits into the corresponding target slots, he is authenticated.

Step 4: If the password is wrong, we will get the forget password the security question which we have registered is displayed in forgot password enter the correct answer for that question the password that we have saved is sent to the registered number.

Image Capturing

If anyone sees our generated one time password and then they try to retype and unlock any app, then their image will be captured and sent to registered mobile number. So misusing of our mobile by others can be easily identified.

Fig. 3. Haptic based security lock screen

Analysis of LOC-happin

- For 1_2 & 3_4:
- The success probability of observation attacks, denoted by poa (1_2& 3_4), is
- poa 1_2 & 3_4 10^4
- For 4_3 & 2_1:
- The success probability of observation attacks, denoted by poa (L_E& H_O), is
- poa 4_3 & 2_1 10^4

COLLECTED RESULTS

We analyzed the collected data from our experiments and surveys to evaluate the effectiveness of the proposed sys-tem. The results are presented in two perspectives: accuracy and usability. The accuracy perspective focuses on the successful login rates in both sessions, including the practice logins. The usability perspective is measured by the amount of time users spent in each Loc-HapPIN phase. The results of these two analyses strongly suggested that Loc-HapPIN is practical to use. At the end of this section, we also presented the statistics of the survey data from participants about their personal background and user experience on smart phones and Loc-HapPIN.

Accuracy

In the apply part of the primary session, participants practiced the login method on a mean of four times starting from one to 14(excluding one outlier) and so emotional onto the authentication (login) part. we have a tendency to outline 2 terms 1st Accuracy and Total Accuracy that were employed in our experiment: Table one shows the

primary Accuracy and also the Total Accuracy of the apply and login phases in each sessions with thirty participants. The result shows that each and Total Accuracies within the first session are beyond those within the second session. Within the 1st session, twenty six out of thirty (86:67%) participants were ready to log into the system with success with only one attempt to all of them were attested among six tries (i.e., the whole Accuracy is 100%). once over fortnight (for a mean of 16:3 days).

The primary Accuracy within the second session was right down to 66:67%, however the whole Accuracy remains 93:33%. We have a tendency to survey the participants for the attainable reasons of the large come by the primary Accuracy and conjointly analyzed those failing login tries within the 2nd session. We have a tendency to notice that the participants failed to very forget their passwords. Most of them still bear in mind the locations of their pass-squares. However, they accidentally shifted the horizontal or vertical bar to a wrong position and submitted on faith .Most of them might log into the system with success within the terribly next attempt to that's why the whole Accuracy (93:33%) is way beyond the primary Accuracy (66:67%) within the second session. Table a pair of shows the typical range of re-tries till the user finally logged in with success.

Usability

The user must bear in mind associate 4-digit PIN in LTM and quickly bear in mind one pass-letter for every login stage. In the challenge state of every stage of the login part, the user will simply and quickly sense the vibration pattern from the 5 contact points. Within the response state of every stage of the login part, the decimal digits from 0 to 9 square measure consecutive allotted within the slot. So that the user will quickly realize the digits of his PIN. The user will simply digits the digits among the letter-digit table. The user doesn't have to be compelled to click a button to let the system proceed to succeeding step, the user's login time are often reduced. Table three shows the period of time that participants consumed within the registration section. The registration took one minute and forty six seconds on the average.

Although it appears the typical registration time could be a bit extended in records, 73:33% of participants felt that the registration method is actually not time intense and 100 percent of them aforementioned that they spent most of their registration time to find pass-squares that are meaningful to them. Supported the survey knowledge from participants, we have a tendency to all over that the time needed for registration is appropriate to users in follow. The specified time to log into Loc-HapPIN is reduced by 16:55 seconds when active four times on the average to urge aware of the shifting (i.e., dragging and flinging) operations on bit screens.

The results are sensible because of the actual fact that 73 of participants have either no or but one year of expertise of mistreatment good phones. What is more, even when over period of time (16:3 days on average), the typical login time was still as low as 37:11 seconds, shortly aloof from that (31.11 seconds) within the initial session. The rationale that the time was slightly augmented was as a result of participants required to recall their passwords.

A survey showed that the time spent within the login method is appropriate to 83:33% of participants. They felt that outlay a touch bit additional time is worth it if the authentication system will defend their passwords from being seen by others peeking over their shoulders.

For the shifting operations, whereas orientating a login indicator to a digit in every vibration there's no important distinction ($F=3:6$, $p> 0:05$) within the range of such operations within the follow section and within the login innovate each sessions, wherever F suggests that the F-test (http://en.wikipedia.org/wiki/F-test) and p suggests that the p- value (http:// en. wikipedia. org/wiki/P-value). As a result of the login indicator is every which way generated for every vibration and components in each the exerciser and vertical bar also are every which way shuffled, the amount of shifting operations wont to move the login indicator to the proper position could dissent additionally. There are 2 styles of shifting operations, that are dragging (aligning the login indicator with the pass-square during a single move) and flinging (fast finger movement on the screen; solely shifting one unit at a time). As shown within the

experimental results, participants solely shifted four to five times per vibration on the average. In summary, the experimental results showed that everyone s participants will operate the login method through the haptic pin authentication interface.

CONCLUSION

With the increasing trend of net services and apps, users are ready to access these applications anytime and anyplace with numerous devices. So as to guard users' digital property, authentication is needed on every occasion they struggle to access their personal account and information. However, conducting the authentication method publically would possibly lead to potential shoulder aquatics attacks. Even a sophisticated secret are often cracked simply through shoulder aquatics. Victimization ancient matter passwords or PIN methodology, users have to be compelled to sort their passwords to certify themselves and therefore these passwords are often disclosed simply, if somebody peeks over shoulder or uses video devices like cell phones.

To overcome this downside, we tend to plan a shoulder surfing resistant authentication system supported somato sense feedback. Employing a one-time registration, users will produce secured login. Recently, touch screen devices giving localized somato sense feedback are designed. It's probably that touch screen devices providing localized somato sense feedback are going to be obtainable for common users within the close to future.

Herein, we've got planned a replacement observation attacks resistant 4-digit PIN-entry theme, Loc-HapPIN, for touch screen devices providing localized somato sense feedback. By victimization the technology of localized somato sense feedback, the usability and also the resistance to observation attacks are improved. We've got shown that Loc-HapPIN can do each sensible security and high usability for general environments**.**

REFERENCES

[1]. V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," Proc. 2004 11th ACM Conference on Computer and Communications Security, 2004, 236-245.
[2]. M. K. Lee, "Security notions and advanced method for human shoulder-surfing resistant PIN-entry," IE
[3]. EE Transactions on Information Forensics and Security, 9(4), 2014, 695-708.
[4]. D. Luca, K. Hertzschuch, and H. Hussmann, "ColorPIN: Securing PIN entry through indirect input," Proc. CHI 2010, 2010, 1103-1106.
[5]. P. Shi, B. Zhu, and A. Youssef, "A rotary pin entry method resilient to shoulder-surfing," Proc. 2009 International Conference for Internet Technology and Secured Transactions, 2009, 1-7.
[6]. T. Kwon and S. Na, "SwitchPIN: Securing smartphone PIN entry with switchable keypads," Proc. IEEE Int. Conf. Consumer Electron., 2014, 27-28.
[7]. Mrs. Aakansha S. Gokhale, Vijaya S. Waghmare, The Shoulder Surfing Resistant Graphical Password Authentication Technique, Procedia Computer Science, 79, 2016, 490- 498.
[8]. Suo, Xiaoyuan, Ying Zhu, and G. Scott Owen. "Graphical passwords: A survey." Computer security applications conference, 21st annual. IEEE, 2015.
[9]. N. Wakabayashi, M. Kuriyama and A. Kanai, "Personal authentication method against shoulder-surfing attacks for smartphone," 2017 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV 2017, 153-155.
[10]. Xingjie Yu, Zhan Wang, Yingjiu Li, Liang Li, Wen Tao Zhu, Li Song, EvoPass: Evolvable graphical password against shoulder- surfing attacks, Computers & Security, 70, 2017, 179- 198.