Random Graphic User Password Authentication Scheme in Mobile Devices

Sung-Shiou Shen[2,a], Tsai-Hua Kang[2,b], Shen-Ho Lin[2,c] & Wei Chien[1,d,*]
[1]Qinzhou University, [2] De Lin Institute of Technology
[a]shaka.kang@msa.hinet.net, [b]3shubert@googlemail.com, [c]marcular@gmail.com, [d]air180@seed.net.tw,

Abstract

Smart mobile terminal are an essential device in our life today. The user usually enters in the related words or draws a simple graphic on the touch screen as passwords for unlocking the screensaver. Although this way can provide users with simple and convenient security mechanism, the process would increase the risk of words or graphic information leakage under the strict security consideration. Usually for this type of keypad lock screen app you can only customize the simple pattern or swipe-to-unlock screen with a static image on a background image that you select to unlock your phone. Therefore, the interested parties could have a chance to eavesdrop the simple graphic pattern information in order to hacking the smart device for stealing the personal information.

Due to lack of the proper identity authentication mechanism in the usually keypad lock screen app, this paper proposes a new graphic pattern protection mechanism for enhance authentication level in the keypad lock screen app field. By randomly changing the fixed position of the digital graphics that shows on the touch screen, the user can draw different graphic pattern every time based on the unique or backup PIN password to unlock the screen. Not only added the random graphic pattern authentication method indeed increase the personal secret information being stolen difficulty and complexity, it provides more security level than the traditional graphic pattern authentication in keypad lock screen as well.

Key words: Authentication, Password, Security, Smart Phone.

Introduction

Nowadays, mobile devices like smartphones and tablets can be found everywhere, they are truly ubiquitous. Interestingly, various private and sensitive data is either stored on the device or can be accessed with it. Moreover, if the mobile device is unlocked, it is also easy for sophisticated attackers to steal the owner's sensitive information, such as identity, account and phone calls. As a sequence, the access to the mobile device has to be secured and user authentication is an indispensable part of mobile interaction today.

Typical countermeasure to protect the user against these attacks is user authentication mechanism. Most deployed authentication methods are based on challenge and response. Meanwhile, modern mobile devices are heavily graphic-oriented, and touchscreen feature is often the primary input method. With the advanced functionalities and interoperation, textual passwords and graphical passwords are the most common means of authentication in mobile devices. Typically textual passwords are strings of letters and digits. Weak passwords have the disadvantage of being vulnerable to dictionary attacks and brute force. Common precautionary approach is mostly increasing the length of the password number, complexity, or periodic replacement password or graphics to guard against. Unfortunately, as mobile devices are often used in public and the input user's password can easily be exposed and observed by the user's vicinity attacker. Such direct observational attacks are called shoulder surfing.

With the advantage of being well-suited to remember graphical information for the human brain, an alternative graphical passwords authentication have been proposed instead of textual passwords for making more user-friendly passwords while increasing the level of security. Graphical passwords presumably offer better usability than textual passwords while keeping the same level of security. Although graphical authentication has advantages compared to password methods, however the shoulder surfing problem is still hidden security threats. Another common problem is that it takes longer time to input graphical passwords than textual passwords due to the differing in consisting of handwritten designs.

As considering the shoulder surfing problem with text based password and longer processing time problem with graphical password systems, a new random graphical password based authentication which is a combination of text password and graphical password based techniques. The proposed scheme is similar to the hybrid system that is based on the text based password (PIN authentication) but also uses tactile one-time pads of graphical password. The novel authentication scheme consists of two phases. The user has to pre-set a textual password and pre-store in the mobile device memory in the first phase called Registration phase. Then a use allows drawing their graphical password on a two-dimensional 3 X 3 grid using one or more lines. During the second phase called Authentication phase, the user has to draw the graphical password correctly and presumably prove the legitimacy of their identity. Authentication phase can provide the strong protection against shoulder surfing attack because of the uncertainty of digit number position in 3 X 3 grids which generated one-time graphical password pattern. Meanwhile, the user verification graphical pattern can be calculated in advance by the mobile device for shorting the processing time.

The rest of the paper is organized as follows. In Section II, we summarize the classification of current graphical password authentication methods. In Section III, the proposed scheme architecture and design process are described. Finally the demonstration of the proposed scheme is shown and a conclusion is given in section V.

Related Work

A smartphone or a mobile phone with an advanced operating system support many useful applications to promote normally work [1]. These applications typically combine the features of a cell phone with those of other popular functions, such as personal digital assistant (PDA), media player and Global Positioning System (GPS). Nowadays, most smartphones can access the Internet. They have a touchscreen user interface and can run third-party apps, music players and are camera phones in the meantime. Therefore, Smartphones run complete operating system software providing a platform for application developers. However, the growing popularity of wireless technology may have finally attracted enough hackers to make the potential for serious security threats a reality [2][3][4]. Furthermore, if you lose your smartphone, there can be outflows of personal and business information. Therefore, authentication scheme is necessary way to identify smartphone's user and to protect the information saved inside the phone. There are many popular authentication methods with smartphone. Slide Lock is provided on Android and IOS system. Slide Lock is a simple and clean locker with powerful notification features. It is weak for security. Typically, keypad, there are ten numbers since 0 to 9 arrange in two dimension array, is used for anyone who deals with numbers frequently. Keypad scheme require a fixed number as password normally. However, this is a tradition method, there are many papers have proved that keypad scheme is weak scheme on authentication. Biometric authentication, finger scan, face scan or iris scan is a type of system that relies on the unique biological characteristics of individuals to verify identity for secure access to electronic systems. However, there are some problems of biometric authentication with smartphone. First problem is the data source which imported into smartphone to identify the user. Smartphone can not to make sure natural data then make a wrong decision.

One deformed password, Pattern screen-lock, reduces repetitive touching and provides for easy dragging [5]. This agreement will safeguard the private smartphone from illegal user interference. However, if users enter an easy pattern for convenience, there is weak security power. Separately, when user touches and drags one dot at a time to make a pattern as password that leaves a trace on the screen. This trace will support hacker to guess the pattern and break the protection. A solution increases another parameter, like acceleration sensor, difference way input from Pattern screen-lock [6]. Since the input signal generated by sensor relate to the user so they can be used to identify the user. However, when legal user shakes the phone, hacker can see and reproduce the action easy. So this is not a strong way to prohibit from attack.

Proposed Graphic User Password Authentication Scheme

In practice, Android is the most popular operating system (OS) and presumably the most widely deployed on smartphones or tablets today. In Android system, Graphic Password Authentication Scheme is so called Android Unlock Pattern scheme which permit a user drawing a sequence of lines connecting the points on a two-dimensional 3 X 3 grid as the user's secret to verify the identification legitimacy. As considering user-friendly, widely-deployment, and robust authentication, the proposed scheme is based on the Android Unlock Pattern scheme with adding the functions in random grid pattern generation and graphic pattern verification. The related software design flow consisted of the following steps and the flow chart is shown in Figure 1 and Figure 2 in detail.

- STEP 1 Registration State: In Android Unlock Pattern scheme, a user must pre-set a 4-8 digit number in a conventional manner as the secret sharing with the database in the mobile device.

- STEP 2 Initial State: When a user touches on sensitive screen to unlock the protection screen in order to log in a mobile device, Android Unlock Patterns with the Random Graphic Grid Pattern Generation is launched in sequence.

- STEP 3 Random Graphic Grid Pattern Generation State (A-B Point): The flow chart shown in Figure 2 is used to generate random Recognition Grid Pattern. Running a specific self-development algorithm to generate 9-digit number random positions is able to merge to different Recognition Grid Patterns while Random Grid Pattern Generation State occurs. The random two-dimensional 3 X 3 grid pattern is the main difference with Android Unlock Pattern. Further, the mobile device has the ability to pre-process one-time authentication grid pattern referring to the pre-stored passwords for saving graphic pattern processing time in case of the hardware limitation. Meanwhile, one-time authentication grid pattern can temporarily pre-store in the database for the follow-up authentication process.

- STEP 4 Authentication State: During this step, a new random graphic grid pattern is displayed to the user who must draw their own password in the same grid pattern and in the same sequence in a conventional operation manner. While the system gets the input and merges the strokes in the user drawn sketch, the user will be authenticated only if the drawn sketch is fully matched with the template pre-stored one-time Authentication Grid Pattern in the database. If authentication is failed, then the state is back to Random Graphic Grid Pattern Generation State (STEP 3) which reproduces new one-time Recognition Grid Pattern and Authentication Grid Pattern, and move on to the next Authentication step (STEP 4). Otherwise, the screen is Unlock.

As finishing the usage of the mobile device, Android Unlock Pattern scheme will be activated for locking the screen again. SETP 2 to STEP 4 procedures will be triggered in sequence when a user tries to access the system again.

 ISBN 978-1-5090-4897-7

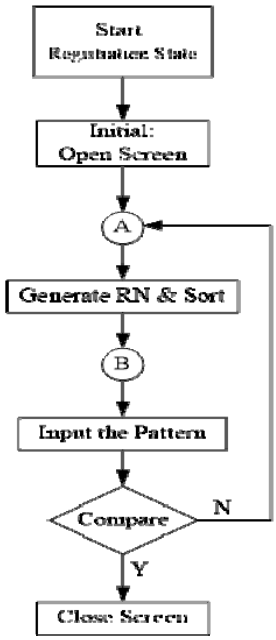

Figure 1 Software Design Flow Chart

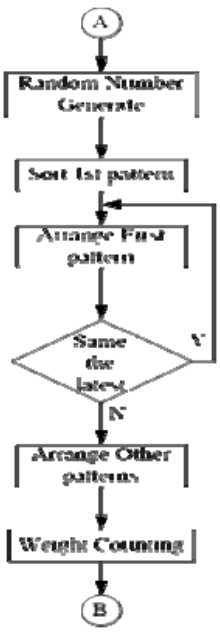

Figure 2 Random Graphic Grid Pattern Generation Flow Chart

Implementations and Conclusions

Figure 3 shows the graphic user interface of self-development keypad lock app which starts up while the user try to unlock the screen. First, the implementation of random number generator algorithm generated random numbers is use to determine the arrangement of each digital buttons on the screen position. For example, if a user password is set to "168", the user must consider the password sequence and the shortest path based on each digital buttons on the screen position. Although the app program is determined mechanism for the shortest path and the password sequence, it offers 1-2 redundant toleration digitals analyzing mechanism for the convenience of users. In other words, the exactly graphic user password is the sequence of "1968". The sequence of "19368" and "17368" both are the tolerate graphic user passwords.

The weight of shortest path calculation is show in Figure 4, the number in the box represents rows and columns position and the weight. The digital number above the line between two boxes represents the different weight of two positions. The entire weight of the path is accumulated different weight value between boxes based on the path order. Meanwhile, the smallest weight value of all kind of possible paths is selected as the shortest path represented the exactly graphic user password pattern.

Today, many user authentication methods and techniques are available in different mobile devices but each with its own advantages and shortcomings. Using graphic based passwords authentication is a growing interest rather than text passwords. Although the proposed scheme in this paper has the advantage with the lock screen digital sequence of random change, even the constant password condition, each time the total number of digitals and graphic user password patterns are different. Indeed, the proposed mechanism overcomes conventional problems of the shoulder surfing and time-consuming authentication process but it has also some limitations and issues like all other graphical based password. Currently we are working on the implementation and evaluation in user adoptability and usability friendly. In future, some other related parameters like time weight factor, image input time interval and user habits will be considered in the proposed scheme to be more secure, reliable and robust.

Figure 3 The graphic user interface of self-development keypad lock app.

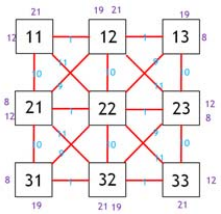

Figure 4 The weight of shortest path calculation

References

[1] Andrew Nusca, "Smartphone vs. feature phone arms race heats up; which did you buy?" ZDNet. Retrieved December 15, 2011.

[2] McAfee, "Mobility and Security: Dazzling Opportunities, Profound Challenges," Technical report, May 2011.

[3] W. Jeon et al., "A Practical Analysis of Smartphone Security," Proc. Int'l Conf. Human Interface and the Management of Information—Part I, Springer-Verlag, pp. 311-320, 2011.

[4] N. Husted, H. Saïdi, and A. Gehani, "Smartphone Security Limitations: Conflicting Traditions," Proc. 2011 Workshop on Governance of Technology, Information, and Policies, ACM, pp. 5-12, 2011.

[5] P. Andriotis, T. Tryfonas, G. Oikonomou, "A Pilot Study on the Security of Pattern Screen-Lock Methods and Soft Side Channel Attacks," Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks, WiSec'13, Pages 1-6, April 17-19, 2013.

[6] K. I. Shin, J. S. Park, J. Y. Lee, J. H. Park, "Design and Implementation of Improved Authentication System for Android Smartphone Users," IEEE Computer Society, 2012 26th International Conference on Advanced Information Networking and Applications Workshops, pp 704-707, 2012.

[7] Pierre L'Ecuyer, "Efficient and Portable Combined Random Number Generators, " Communications of the ACM, Vol. 31, No. 6, pp. 742-774, June, 1988.

[8] Dr. Paul Coddington, "Parallel Random Number Generators in Java," The University of Adelaide, Australia, November 2, 2003.

[9] Stephen K. Park and Keith W. Miller, "RANDOM NUMBER GEUERATORS: GOOD ONES ARE HARD TO FIN," Communications of the ACM, Vol. 31, No. 10, pp. 1192-1201, October 1988.

[10] M. R. Henzinger, P. Klein, S. Rao, S. Subramanian, "Faster Shortest-Path Algorithms for Planar Graphs," Journal of computer and system sciences, 1997.

 ISBN 978-1-5090-4897-7