석사 학위논문
Master's Thesis

풀 터치 스크린 방식의 스마트 기기에서 어깨 공격에 대응하는 패스워드 입력 방식 연구

A Study on Shoulder-Surfing Resistant Password Scheme for Smart Devices with Full-touch Screen

박 이 재 (朴 珥 材 Park, Yi Jae)
전산학과
Department of Computer Science

KAIST

2012

풀 터치 스크린 방식의 스마트 기기에서 어깨 공격에 대응하는 패스워드 입력 방식 연구

A Study on Shoulder-Surfing Resistant Password Scheme for Smart Devices with Full-touch Screen

A Study on Shoulder-Surfing Resistant Password Scheme for Smart Devices with Full-touch Screen

Advisor : Professor Kwangjo Kim

by

Park, Yi Jae
Department of Computer Science
KAIST

A thesis submitted to the faculty of KAIST in partial fulfillment of the requirements for the degree of in the Department of Computer Science . The study was conducted in accordance with Code of Research Ethics[1].

2011. 12. 20.

Approved by

Professor Kwangjo Kim

[Advisor]

---

[1]Declaration of Ethical Conduct in Research: I, as a graduate student of KAIST, hereby declare that I have not committed any acts that may damage the credibility of my research. These include, but are not limited to: falsification, thesis written by someone else, distortion of research findings or plagiarism. I affirm that my thesis contains honest conclusions based on my own careful research under the guidance

풀 터치 스크린 방식의 스마트 기기에서 어깨 공격에 대응하는 패스워드 입력 방식 연구

박 이 재

위 논문은 한국과학기술원 석사학위논문으로
학위논문심사위원회에서 심사 통과하였음.

2011년 12월 20일

심사위원장 김광조 (인)

심사위원 박진아 (인)

심사위원 이기혁 (인)

---

of my thesis advisor.

MCS
20104193

박 이 재. Park, Yi Jae. A Study on Shoulder-Surfing Resistant Password Scheme for Smart Devices with Full-touch Screen. 풀 터치 스크린 방식의 스마트 기기에서 어깨 공격에 대응하는 패스워드 입력 방식 연구. Department of Computer Science . 2012. 33p. Advisor Prof. Kwangjo Kim. Text in English.

ABSTRACT

A smartphone is considered to a kind of a high-end mobile phone which exhibits of contemporary feature phones and computers with more advanced computing ability and connectivity. The number of the smartphone users in the world has been growing dramatically, and most of smartphones are using Apple's iOS and Google's Android as their operating system depending on the makers. Also, after releasing iPad by Apple, the number of a tablet computer which looks like a small-sized computer is rapidly increasing. The security of smartphones and tablet computers must be more important than the general mobile phones and the traditional computers. Especially, since most of smartphones and tablet computers are using full-touch screen, they have vulnerability against shoulder surfing (attack). However, the existing password schemes of smart devices are not resistant against shoulder surfing at all. In this thesis, we propose and evaluate shoulder-surfing resistant password scheme for smart devices with full-touch screen. We propose three new schemes: the multi-finger PIN pad (Scheme A), the password scheme with the wheels and the shield gesture (Scheme B), and the password scheme using tilt of the devices (Scheme C). By our experiment, we show that our schemes are more secure than the existing password scheme, even though they have longer password input time. In particular, all observers failed to observe the passwords in Scheme B. We expect that our schemes can lead the users of smart devices to more secure use of them.

Contents

List of Tables

List of Figures

Chapter 1. Introduction

1.1 Overview

A smartphone is a kind of a high-end mobile phone which exhibits contemporary feature phones and small-sized computers. In other words, a smartphone looks like a tiny computer with a function of a mobile phone. The popular smartphones also serve to combine the functions of portable media players, digital cameras, high-resolution touchscreens, web browsers that can access and display standard web pages rather than just mobile-optimized sites, GPS navigation units, and high-speed data access via Wi-Fi and mobile broadband.

After Apple's iPhone released into Korean market in 2009, the number of smartphone users in Korea has been growing dramatically. Not only in Korea, but also in worldwide, the number of smartphone users has been increasing steadily [1]. The core of worldwide increase in the number of smartphone users is being occupied by two smartphone operating systems, Apple's iOS and Google's Android. Releasing Apple's iPhone has served as a momentum for the general public to use smartphones regarded as exclusive product to the employees, and Google's Android gave an impact to the popularization of smartphones with its specific advantages: free release, multi-channel and multi-carrier OS.

According to a report [1] by Gartner, Inc., an information technology research firm, in the first quarter of 2011, Smartphones accounted for 23.6 percent of overall sales of mobile phones, the market share of Android in smartphone OS ranked in the first place, and iOS did in the second place. The rest of the representative smartphone OS are RIM's BlackBerry and Microsoft's Windows Mobile. Fig. 1.1 shows the worldwide smartphone OS market share as of the first quarter of 2011.

Beside smartphone, after releasing Apple's iPad in 2010, the number of tablet computer (tablet devices) users is also growing [2]. A tablet computer is a mobile computer, larger than a mobile phone or personal digital assistant, integrated into a full-touch screen and primarily operated by touching the screen. It often uses an onscreen virtual keyboard, a passive stylus pen, or a digital pen, rather than a physical keyboard [3]. Since the market share of iOS and Android in tablet computer OS occupies more than 95% in the second quarter of 2011 [2], the tablet computers can be thought to be smartphones with

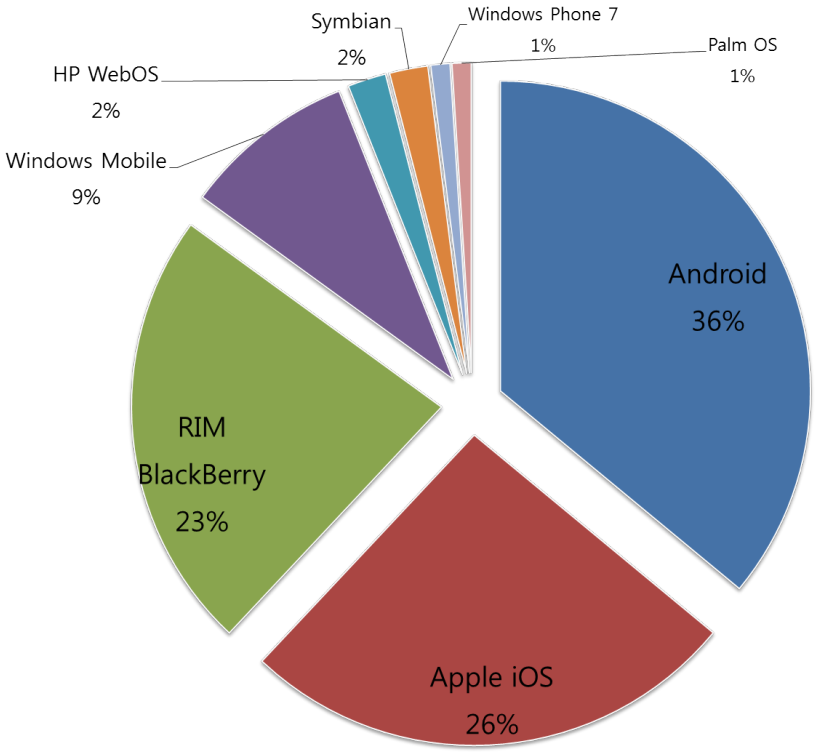

Figure 1.1: Worldwide Smartphone OS Market share as of Q1 2011 [1]

a big screen.

Most of smartphones on the market currently support a full-touch screen for functions of computers (*e.g.* full browsing, *etc.*). By a full-touch screen and requirements for customers for thin devices, most smartphones provides an onscreen virtual keyboard like tablet computers described in Fig. 1.2.

Also, since smartphones have the functions of feature phones and computers, the security of smartphones is more important than one of feature phones. Smartphones keep the privacy-related information (*e.g.* contacts, SMS, phone records, photo, *etc.*) like feature phones and the personal financial information (*e.g.* bank accounts, stock investments, etc.) like computers. For this purpose, smartphones support not only 4-digit PIN of feature phones, but also high-level password like a password scheme using numbers, alphabet, and special characters and pattern-input scheme.

However, because of full-touch screens, smartphones have wider screens and keyboard than feature phones. Then, with these features, smartphones are vulnerable to shoulder surfing. In this thesis, we propose new password schemes which can be resistant against shoulder surfing attacks for full-touch screens of smartphones and tablet devices, compare our schemes with existing password schemes and

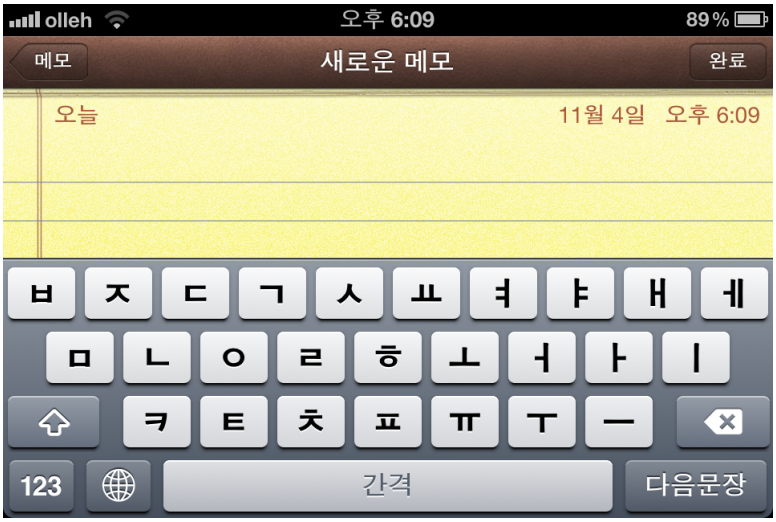

Figure 1.2: Keyboard in Screen of iPhone

evaluate our schemes by experiments.

1.2 Organization

The remainder of the thesis is organized as follows: The background and related researches resistant to shoulder surfing are conducted in Chapter 2. Our schemes and design considerations are presented in a detailed manner in Chapter 3. Chapter 4 discusses conceptual evaluation and introduces evaluation setting by experiment. Finally, we summarize and conclude the thesis in Chapter 5.

Chapter 2. Background and Related Work

2.1 Shoulder Surfing

In computer security, shoulder surfing (attack) is to get information using direct observation techniques, such as stealing over the shoulder who inputs the password into an electric device [4] [5]. Shoulder-surfing happens when an attacker learns a password of a user by watching the user log in. Shoulder-surfing is a popular method of stealing passwords and other sensitive information and has been recognized by practitioners as a serious security threat. It can occur in the offices and the public places without the awareness of a user [24]. Shoulder surfing is particularly effective in crowded places because it is relatively easy to observe someone. The following situations or places are where shoulder surfing attacks happen frequently:

- Enter their PIN at an ATM or a POS terminal
- Enter a password at a cybercafe, public and university libraries, or airport kiosks
- Enter a code for a rented locker in a public place

Shoulder surfing can also be done at a distance using binoculars or other vision-enhancing devices. Inexpensive, miniature CCTV cameras can be concealed in ceilings, walls or fixtures to observe data entry.

Recent ATMs now have a sophisticated display which prevents shoulder surfers from obtaining displayed information. It grows darker beyond a certain viewing angle, and the only way to tell what is displayed on the screen is to stand directly in front of it. However, there are some ATMs which have a PIN pad outside the display. Also, since smartphones and tablet computers can operate like a portable media player, someone can show their display at various angles, and the mechanism used an ATM to prevent this is difficult to apply to smart devices.

2.2 Password Schemes of Smartphone & Tablet Devices

2.2.1 Google's Android

Google's Android is a software-stack containing for mobile devices, operating system, middleware, and core applications. Android basically supports password settings at the screen lock, call, and SIM card access.

Android supports three password schemes. One is the PIN for the screen lock and the call lock, another is the pattern for the screen lock, and the other is the keyboard password for the screen lock and SIM card lock.

The PIN is a method to input more than 4-digit number password. The left picture in Fig. 2.1 is a typical screenshot in which the user sets her/his PIN, this screen is similar with to one in which the user inputs the PIN.

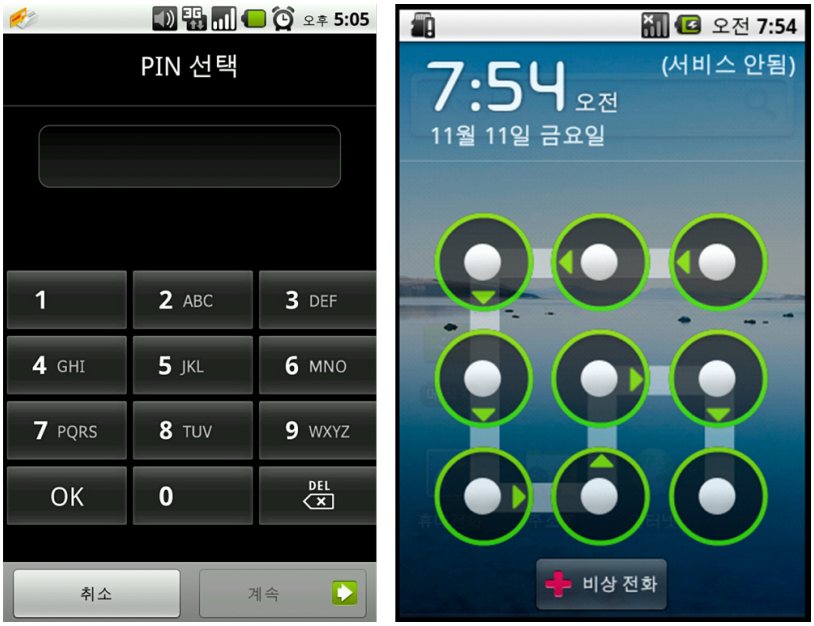

Figure 2.1: Password input in Android (left: PIN, right: pattern)

The pattern is a method to input the password drawing a line connecting the white points. The line can pass a point once for all. The user can select whether the line is visible or not. The right picture in Fig. 2.1 is another screenshot in which the user input the correct pattern password.

The keyboard password in Fig. 2.2 is same as the password in normal computers. All numbers, alphabet, and special characters can be used for password.

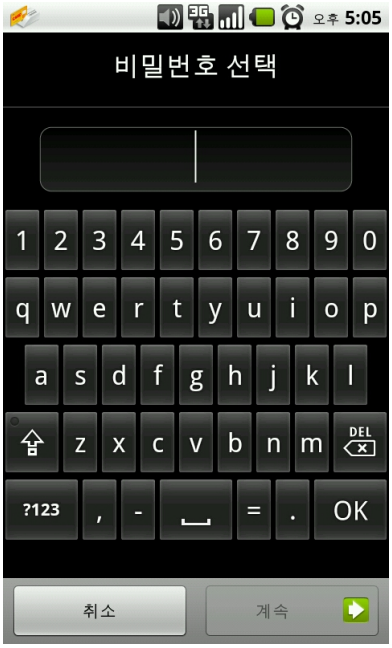

Figure 2.2: Keyboard Password Input Screen of Android

2.2.2 Apple's iOS

iOS developed by Apple is a mobile operating system used for a smartphone - iPhone, portable media player - iPod touch, and tablet computer – iPad made by Apple. iOS is derived from Apples computer OS, Mac OS X 10.5. Unlike Android, iOS supports a password only at the screen lock, basically. For data protection, the user can select the option in which after 10 consecutive input failure, all data in the device may be deleted. Also, the default option is that after the consecutive input failure, data in the device is protected by deactivating the device.

iOS supports two password schemes. One is 'Simple password' in the left screenshot in Fig. 2.3 using a 4-digit number and another is the password using all numbers, alphabet and special characters in the right screenshot in Fig. 2.3.

2.2.3 Bank and Stock Applications in Smart Devices

Most of mobile applications use the password schemes that the operating system provides fundamentally. However, online banking or stock services that must be safer than general mobile applications use the password schemes which are different from traditional ones.

Fig. 2.4 shows the account password input screens of Shinhan bank and Woori bank in Korea. The

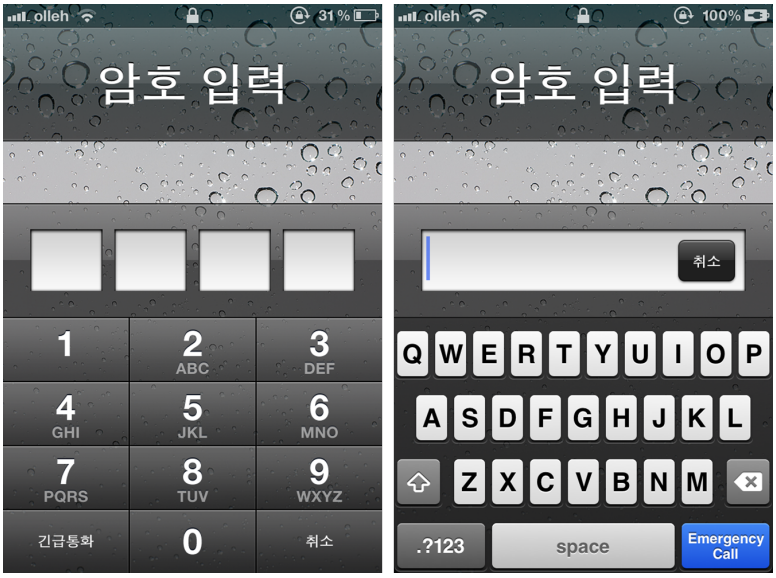

Figure 2.3: Lock Screen with Password of iOS (left: simple password, right: password using all numbers, alphabet and special characters)

Figure 2.4: Account Password Input in Bank (left: Shinhan bank, right: Woori bank)

application of Shinhan bank arranges the numbers randomly. The Woori bank arranges the numbers not randomly, but adds blanks between some numbers. Fig. 2.5 shows the certificate password input screens of two banks. Both applications add blanks between some keys like the account password input screen of Woori bank.

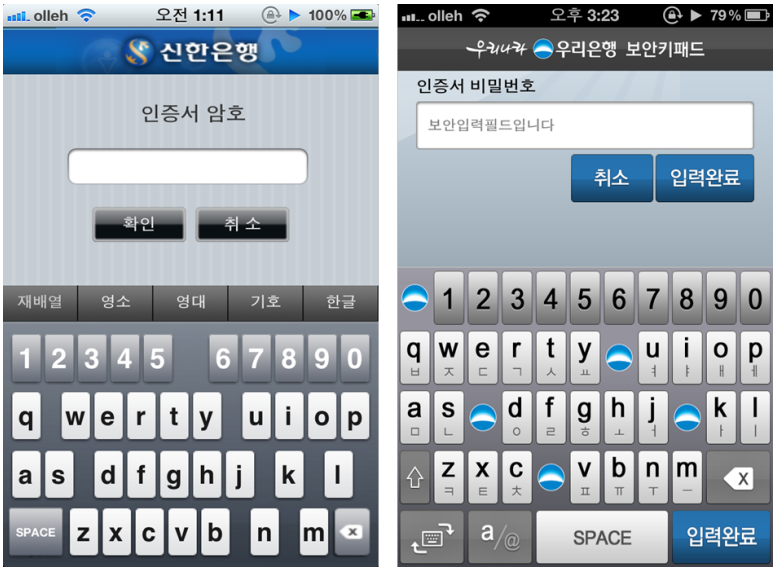

Figure 2.5: Certificate Password Input in Bank (left: Shinhan bank, right: Woori bank)

2.2.4 Windows 8

Windows 8 is the codename for the next version of the Microsoft Windows computer operating system following the previous Windows 7. Like the previous versions, it is for home and business and supports not only personal computers, but also tablet devices like Android and iOS. For tablet devices, Windows 8 adopt PIN pad to input 4-digit numbers as password and 'Picture password' besides the existing keyboard input password.

'Picture password' allows users to sketch in three different places over the picture to login. Users can sketch three actions: dotting, drawing a line, and drawing a circle. Microsoft expects that 'Picture password' become a fast, safe password authentication [7].

2.3 Multi-Touch Authentication on Tabletops [8]

David Kim, *et al.* [8] have introduced a number of novel tabletop authentication schemes that exploit the features of multi-touch interaction in order to inhibit shoulder surfing. They suggested that within the public display or tabletop context, successful authentication rests, not only upon reliable system technology and effective security protocols, but also upon full system acceptability within a social context. The situation to input the password in the public display or tabletop is vulnerable to shoulder surfing. Then, when the users give their password, they can perform the shield gesture or be

very conscious of the people around them. At this moment, these actions can be thought to signal an explicit mistrust of the human-beings. To prevent this misinterpretation, the authors emphasize the social factors.

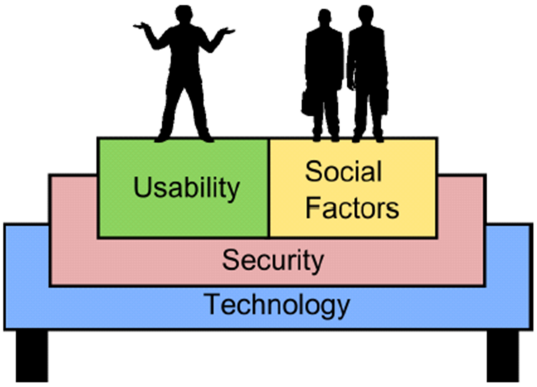

Figure 2.6: Important considerations for security mechanisms in co-located collaborative contexts [8]

The proposed method by D. Kim *et al.* is summarized as follow.

2.3.1 Enhanced PIN Input

ShieldPIN

ShieldPIN in Fig. 2.7 incorporates a compulsory hand shielding gesture that provides a physical barrier to visibility. In ShieldPIN, the password input process is as follow: first, the user performs the shield gesture in the green zone. Upon detection of the gesture, the keypad is displayed behind the shield, and the user can input the password with this keypad. The PIN keypad can appear and disappear in response to the detection of the shielding gesture.

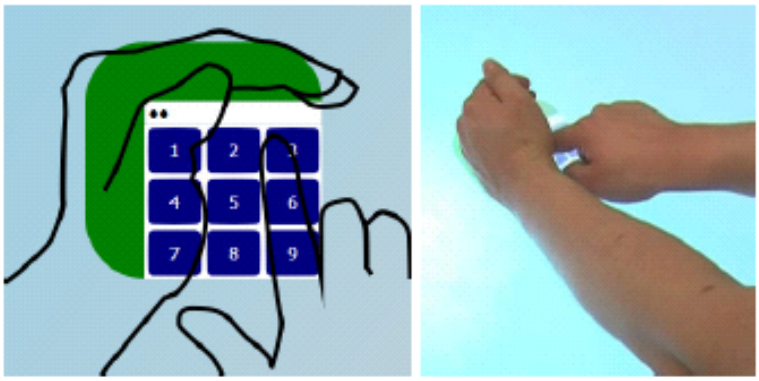

Figure 2.7: ShieldPIN [8]

Since the user must execute the shielding gesture to input the password, the shielding gesture is no longer a voluntary action that could be interpreted as an indicator of mistrust.

By the shielding gesture, the user can block observation from forward and left side, and observation from the side uncovered by the shielding gesture is blocked by the hand entering the password. However, an attacker is most likely to be successful from a vantage point behind the shield.

SlotPIN

The SlotPIN in Fig. 2.8 is based on the principles of providing redundant information and encouraging concurrent actions. The user enters a PIN by aligning reels on the interface with wheels so that one row contains the correct password. The particular row containing the correct password is determined by the first static reel.

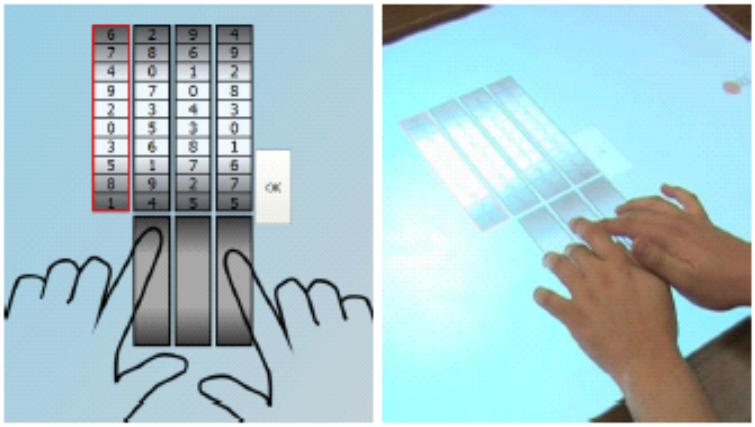

Figure 2.8: SlotPIN [8]

The current form of SlotPIN is immune to one shoulder surfing attack, but has a vulnerability to multiple attacks. The best-case scenario for an attacker is that only 2 observed logins are required for success in identifying the password. After recording the end-state of first login, the attacker has 10 candidate PINs. Observing one further successful login in the best case will enable the attacker to find the PIN that the two logins have in common, this is an intersection attack. For this reason, it is not a suitable deployment where camera-based attacks are of a primary concern.

CuePIN

CuePIN in Fig. 2.9 addresses the vulnerability of SlotPIN to intersection attack by combining features of both SlotPIN and ShieldPIN. CuePIN has the part which the user performs the shield gesture like ShieldPIN, reels and wheels like SlotPIN. Each row is also supplemented with an identifier character in the range A-J, and when the user manipulates each wheel with the shield gesture, the user can see a random character in the range A-J which points what row has the real input. In Fig. 2.9, the real input of the first reel is row C.

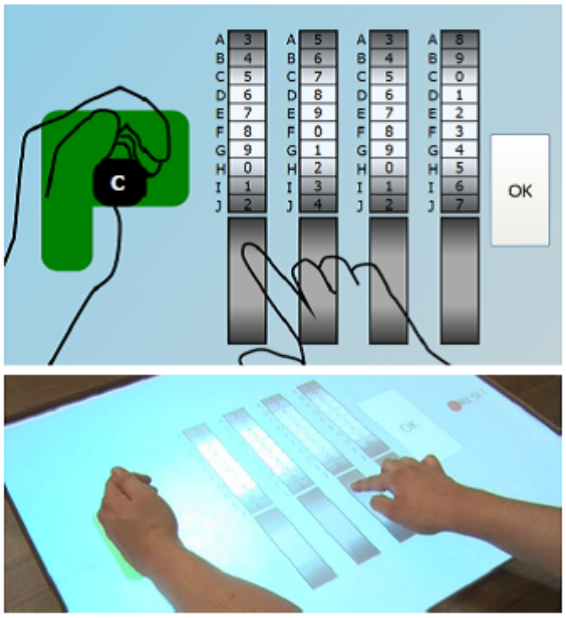

Figure 2.9: CuePIN [8]

In CuePIN, a password entry proceeds as follows: first, the user get the real input of first reel by the shield gesture. If the user removes their hand from the screen, the character disappears. Second, the user manipulates reel i to align PIN digit n to the row revealed by the shielding gesture. Finally, repeat the first action and the second action until the password have been entered.

Since users are required to shield a much smaller area than in ShieldPIN, CuePIN is safer. Also, the addition of the alphabetic characters at each position of the reel enables a random on-screen representation of the password of a user. This method is resistant to multiple shoulder surfing attacks with or without a camera where an attacker fails to record both the shielded cue area and the final reel states. Without the sequence of shielded cues, the knowledge of the end-state cannot be usefully applied in a

replay attack.

2.3.2 Color-Rings

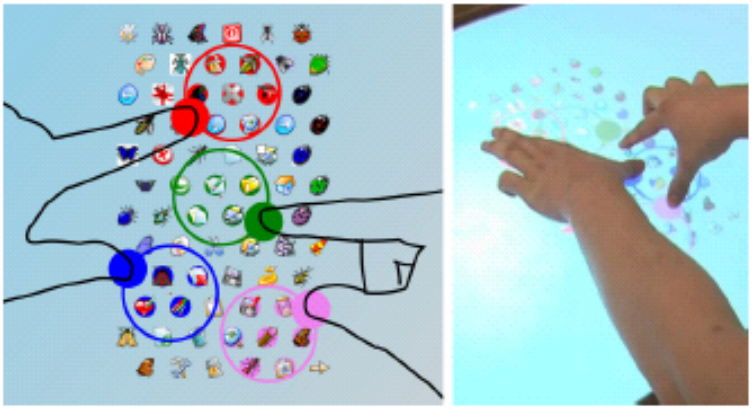

Figure 2.10: Color-Rings [8]

Color-Rings in Fig. 2.10 is a visual authentication scheme that exploits both concurrent and redundant actions. The interface is similar in appearance to the Convex Hull Click scheme [24]. The user is assigned i authentication icons called key icons that are collectively assigned one single color-ring: red, green, blue, or pink. At login the user can see i grids of icons where 72 icons are displayed per grid and one key icon is presented in each. Also at each login the position of the icons is randomized and distinct icons are displayed in each grid.

For each grid the user must select the key icon with the correctly colored ring. The user is asked to place 4 fingers down on the display (ideally index finger and thumb from each hand) around which four rings of different colors are then drawn. The user must drag all 4 rings concurrently and place them in the grid, and three of the rings make decoy selections. Users confirm a selection by dropping the rings in position.

2.3.3 Pressure-Grid

Some recent systems can obtain some changes in finger pressure, but pressure differences are very difficult for observers to discern. Also, since increasing pressure on some fingers (particularly the less dexterous fingers), causes involuntary movement on other fingers, observers become more confused. This principle can form the basis of low-visibility interactions with the system. Pressure-Grid uses this principle.

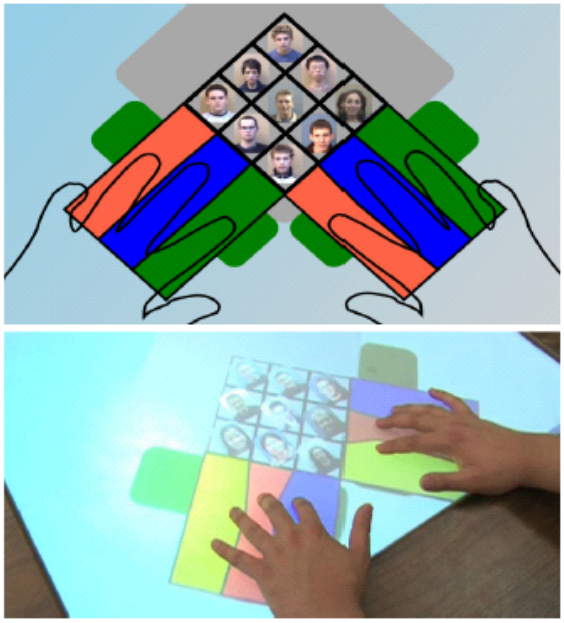

Figure 2.11: Pressure-Grid [8]

Pressure-Grid in Fig. 2.11 is a novel multi-purpose input mechanism that exploits this low visibility of changes in finger pressure for purposes of inputting passwords.

The user begins by placing three fingers of each hand in calibration areas on the interface. The system uses the locations of these touch points to dynamically draw the grid of objects, and pressure zones that are assigned to each finger. To select a particular cell, the user must apply additional pressure on one finger per hand. One additional method used to increase the difficulty of observing finger pressure, is that the pressure zones change color constantly and randomly.

One possible limitation of this system is in terms of accessibility as it requires good dexterity of the hands. Despite this, the authors believe it to be a promising solution to co-located observation attacks and camera attack. However, Marshall *et al.* [9] proposed a camera technique which is used to detect the change in color of flesh beneath the fingernail, this is useful to detect pressure of the finger upon a surface.

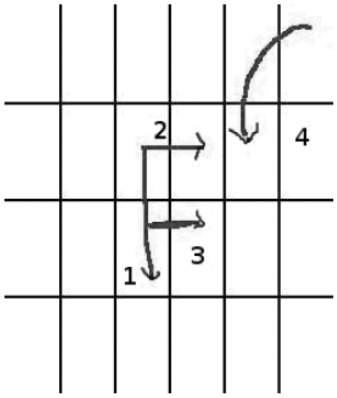

Figure 2.12: DAS [11]

2.4 Multi-grid Graphical Password Scheme [10]

2.4.1 DAS: Draw-a-Secret [11]

Jermyn *et al.* [11] proposed a scheme called Draw-a-Secret (DAS) in Fig. 2.12, targeted for PDA devices. In this scheme, the user draws a design on a display grid, which is used as the password. In the registration phase, the user determines patters for their password. In the authentication phase, the user can start anywhere and go in any direction, but must occur in the same sequence. Each continuous stroke is mapped to a sequence of coordinate pairs, by listing the cells through which it passes.

To avoid ambiguity in cases of strokes that run along the cell boundaries, the size of each cell must be sufficiently large to provide a degree of tolerance when the user draws a password. The authors suggested that the size of the password space for graphical passwords formed using a 5 X 5 grid is larger than that of alphanumeric passwords. Fig. 2.12 illustrates a four-stroke password entry example in a 4 X 6 grid.

D. Nali and J. Thorpe [12] and Goldberg *et al.* [13] pointed out the weak point of DAS. Nali and Thorpe assumed that if the patters are centered or symmetric, the patters are predictable easily. Actually, by the result of the experiment, 86% of users drew centered patterns, 45% drew symmetric patterns, and there are 29% of input failure. Goldberg *et al.* showed that humans are less likely to recall the order in which they drew a DAS password than the complicated passwords (non-dictionary words, numbers, and special characters).

2.4.2 Multi-grid DAS [10]

In order to solve the weak points of DAS mentioned previously, Chalkias *et al.* [10] proposed Multi-grid DAS which is a different modified DAS where the cells are not identical in size. The authors made cells of various sizes using a multi-grid (internal grids) construction. The aim of this scheme is to decrease the password centering effect. Fig. 2.13 is an example of a password in Multi-grid DAS, and Fig. 2.14 is a template of Multi-grid DAS.

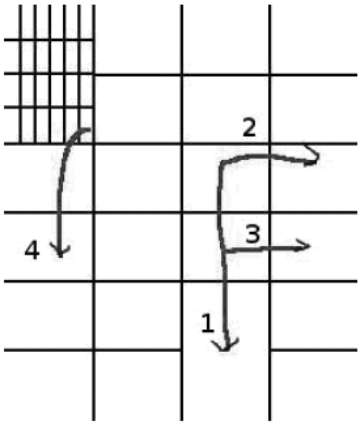

Figure 2.13: Multi-grid DAS [10]

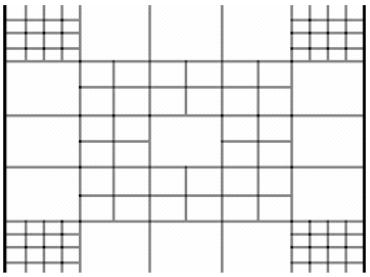

Figure 2.14: A Multi-grid DAS Template[10]

Another strong point of Multi-grid DAS compared with DAS is that it can decrease password input errors. In DAS, the main reasons that users fail to repeat their password relies on the fact that they forget their stroke order (ordering errors) or they mark adjacent cells and not the correct ones (shift errors). The authors showed that the number of shift errors was larger than ordering errors and Multi-grid DAS can reduce the number of shift errors. Also, because of the cells of the various sizes, observers are difficult to observe the passwords by shoulder-surfing.

Chapter 3. Our Scheme

3.1 Design Considerations

In practice, shoulder surfing can be hampered by interfering with one or more steps in the processes of sense making and knowledge acquisition for an observer [8]. These can be summarized as follows:

3.1.1 Reduce visibility

This method reduces the saliency of areas on a display where sensitive actions take place. This can be achieved through additional hardware (*e.g* optical filters), forcing the user to cover input, computer graphics techniques (*e.g.* reduced visual quality, exploitation of orientation).

3.1.2 Subdivide action

This method subdivides the input action temporally or spatially and performs sub-actions sequentially (or concurrently when the action is divided spatially). In this way, the one-to-one mapping between one action and one part of the authentication key is removed, making actions harder for an observer to decipher due to lacking knowledge of user intentions.

3.1.3 Dissipate attention

This method displays redundant information to hinder the observer identifying information on the interface that is useful to memorize easily. However, the use of redundant information can negatively impact usability as the user must also navigate this information. Such systems are vulnerable to intersection attacks where an attacker records multiple logins and collates them in search of recurring patterns that can be used to uncover the credentials.

3.1.4 Knowledge transformation

With this method, the user enters the credentials in a form that is difficult, in isolation, to be used to reconstruct the correct credentials after observing a successful login. A key concern is that the transformation must be usable without excessive calculation from a user.

3.2 Our Scheme

In this section, we propose 3 schemes for full-touch screen environment of smart devices, which reduce the possibility of shoulder-surfing.

3.2.1 Scheme A - Multi-fingers PIN pad

In Scheme A (Fig. 3.1), to input the password, the user uses her/his two or more fingers not a finger. Scheme A is similar to the standard PIN pad, but different since it has symbols in addition to numbers.

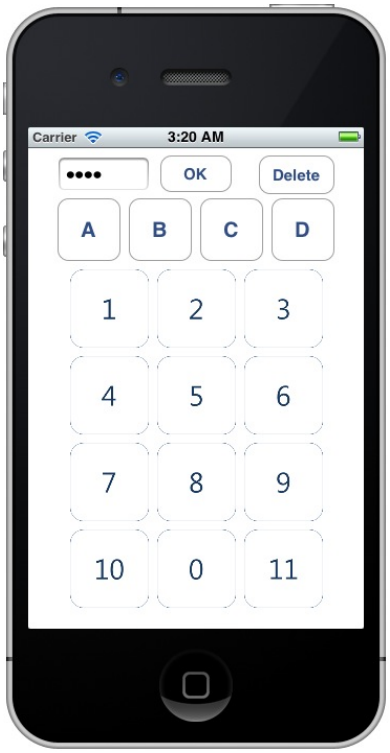

Figure 3.1: Scheme A

In Scheme A, the input of the password is composed of pressing one or more numbers and a symbol with two or more fingers. The symbols have following functions:

- Normal: The entered number in company with this symbol is inputted intactly. The scheme ignores the input if two or more numbers are entered with this symbol.
- Plus: Scheme A adds the entered two or more numbers, processes the result of the addition with the option, and accepts the processed result. The options are 'Enter the unit digit of the addition'

and ‘Enter the addition intactly’, and the user selects an option.

– Multiply: Scheme A multiplies the entered two or more numbers, processes the result of the multiplication with the option, and accepts the processed result. The options are ‘Enter the unit digit of the multiplication’, ‘Enter tens’ digit of the multiplication’, and ‘Enter the multiplication intactly’, and the user selects an option.

– Ignore: Scheme A ignores the entered number(s) with this symbol.

For instance, let ‘A’ be ‘Normal’ symbol, ‘B’ be ‘Plus’ symbol, ‘C’ be ‘Multiply’, and ‘D’ be ‘Ignore’ symbol. Also, we assume that the user selects the option ‘Enter the unit digit of the result’ for both ‘Plus’ and ‘Multiply’, and the password is 1234. Then, the user can input the password like following examples (in these examples, ’+’ means simultaneous input):

– 1+0+B, 1+2+C, 3+A, 1+3+B

– 3+7+C, 2+A, 8+7+D, 3+0+B, 1+4+C

There are other various examples besides the above two examples.

However, in Scheme A, there can be a problem that the user always inputs the password on the same way. Then, we propose another mode of Scheme A.

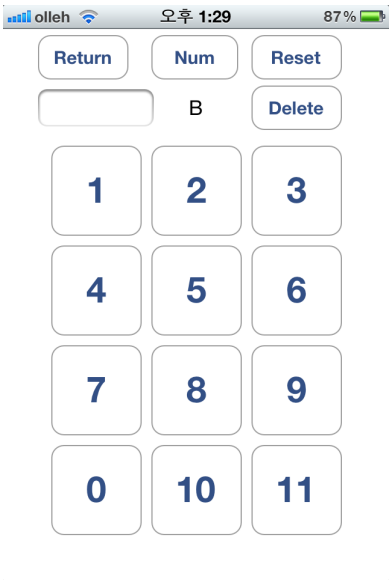

Figure 3.2: Another Mode of Scheme A

In order to solve the above problem, the entered symbol with numbers can be selected by the system randomly, not the user (Fig. 3.2). The system shows randomly 'Normal', 'Plus', 'Multiply', or 'Ignore' symbol, and the user inputs one or more number(s) accordingly. In the experiment, we used this mode of Scheme A.

3.2.2 Scheme B - Enhanced CuePIN

Scheme B in Fig. 3.3 is a method which applies CuePIN of D. Kim *et al.* [8]. We propose Scheme B in order to solve the weaknesses which are that CuePIN takes up much space to input a long password and the length of passwords is fixed in CuePIN.

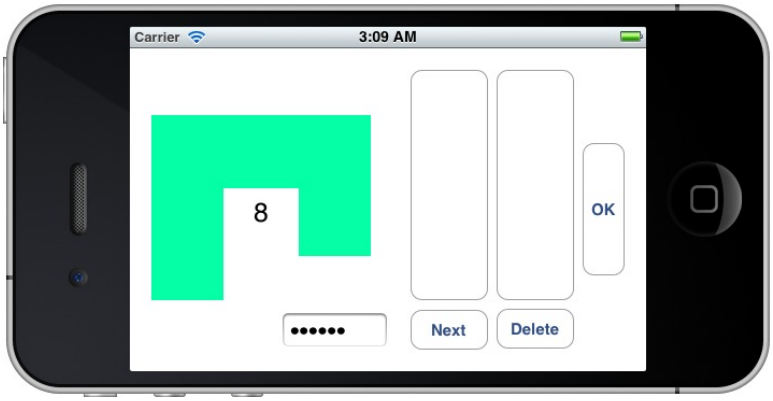

Figure 3.3: Scheme B

In Scheme B, there is a defined area to perform the shield gesture like CuePIN and two wheels which the user can rotate with her/his finger. However, unlike CuePIN, Scheme B has no row identifier characters (A-J) and reels showing digits. Instead, the area under the shield gesture shows alphabet, digits, or special characters which the wheel touched by the user points. Scheme B has two wheels. The default options is that the left wheel has 26 letters of the English alphabet, and the right wheel has digits (0-9) and special characters which include 'shift' for capital letters and Korean-English button. Also, there are the 'next' button in order to input a multiple-digit password, the 'del' button to delete wrong input, a space in which the user can confirm the digit of the password, and the 'OK' button.

With the shield gesture, like CuePIN, the element of the wheel appears, and if the user removes her/his hand from screen, the element disappears.

The password input process of Scheme B is as in the following:

1. The user performs the shield gesture in a defined area.

2. If the user turns the left wheel, the characters of the left wheel appear on the shielded area, or if the user turns the right wheel, the characters of the right wheel appear on the shielded area. The user enters the character of the relevant wheel for the password and press 'Next' button.

3. Repeat steps 1 and 2 until all passwords have been entered, and press 'OK' button.

Scheme B can have following additional functions: first, when the user selects a wheel, the first character appears randomly. If the first character is fixed, with the duration of turning the wheel, the observer can guess what the user inputs. Second, the user can change the characters of two wheels. Our default option is that the left wheel has the English alphabet and the right wheel has digits and special characters, but the user can change these.

The user are required to shield a much smaller area since only a single character is revealed and this improves the secrecy of the shielding gesture in Scheme B. Also, there is no limitation of length of passwords in Scheme B.

3.2.3 Scheme C - Using tilt

iOS from iOS 4 and Android from Gingerbread (version 2.3) support the gyroscopic function if a device operating under iOS or Android has a gyroscopic sensor. With the gyroscopic function, the measurement and maintenance of the slope or direction of the device become more accurate. From this, users of smart devices can enjoy more convenient augmented reality applications and game applications. Scheme C, with this gyroscopic function, is a method of inputting password using the slope of the device.

In Scheme C, there is a defined area to perform the shield gesture, and when the inputter shields this area with her/his left or right hand, the numbers appears. The arrangement of numbers is random. Based on this arrangement of number, the inputter enters the password tilting the device. For example, in order to input 2 in Fig 3.4, the inputter touches the screen, tilts the device forward, and then tips it to the right.

The password input process of Scheme C is as in the following:

1. The user performs the shield gesture in a defined area.

2. The user memorizes the arrangement of numbers which appears after the shielding gesture.

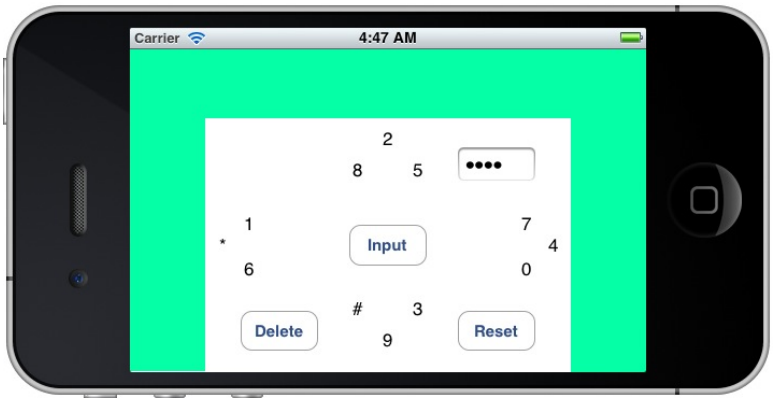

Figure 3.4: Scheme C

3. The user removes their hand from the screen of device, and then the arrangement of numbers disappears.

4. The user inputs its own password, pressing the 'Input' button and tilting the device.

5. Repeat step 4 until all password have been entered.

If the observer failed to observe the area under the shield gesture, the tilting processes which she/he observed are useless. Also, we expect that the tilting processes are indistinguishable by the observation.

Chapter 4. Evaluation

4.1 Conceptual Evaluation

Based on 4 design considerations of chapter 3.1, we can conceptually evaluate the schemes we proposed in Table 4.1. In table 4.1, * (primary) means a primary providing function of the scheme, and + (supporting) means a function which the scheme is able to support in addition.

Scheme A provides 'Subdivide action' basically, with inputting numbers and a symbol at the same time. Also, it provides 'Knowledge transformation' basically, with a computation of numbers and a symbol. It can support 'Dissipate attention', when users input their password, they use the 'Ignore' symbol.

Scheme B provides 'Restrict visibility' with the shield gesture of the user in a defined area. Since a character which is a part of the password is under the shield gesture, and the user changes it using reels, 'Subdivide action' is provided. 'Knowledge transformation' is provided with the control of the user for reels. Also, by showing other characters on reels, 'Dissipate attention' can be supported.

Scheme C provides 'Restrict visibility' with the shield gesture in common with Scheme B. Also, since the part which shows numbers and the password-input step are divided, 'Subdivide action' is provided. To input password with tilting the device is 'Knowledge transformation'.

Table 4.1: Shoulder surfing resistance methods of proposed schemes

	Restrict visibility	Subdivide action	Dissipate attention	Knowledge transformation
Scheme A		*	+	*
Scheme B	*	*	+	*
Scheme C	*	*	+	*

4.2 Experimental Setting

We referred to the experimental methods of D. Kim *et al.* [8] and F. Tari *et al.* [14].

1. Criteria

We evaluated 3 schemes with the following criteria.

- Input time: The duration when an inputter input passwords. It is from first input to last input.
- Input accuracy: Ratio of number of password inputs of users to exact password inputs.
- Imitability: Percentages of observers able to replicate the inputter's passwords
- Response of participants: The participants were given a post-experiment questionnaire.

2. Devices

   We used Apple's iPhone 4 for a smartphone and iPad2 for a tablet computer.

3. Participants

   30 participants were recruited to take part in the study. They are undergraduate and graduate students of KAIST Computer Science Engineering and Electrical Engineering.

   The age mean for the participant group was 23.77 with a standard deviation of 1.52. All participants had their own smartphone or tablet computer and indicated their level of expertise with smart devices as expert.

4. Passwords in the Experiments

   The participants input the passwords (4-digit number) in the proposed schemes and the existing password schemes.

5. Procedures

   The procedure was as follows:

   (a) Participants were invited to training session, the protocol of the experiment was explained, and given time to familiarize themselves with each of the 3 schemes.

   (b) A group consists of 3 participants. One participant was randomly given the role of inputter for the entire session, while the remaining two were assigned as observers (attackers).

   (c) The observers left for a moment. The inputter chose an authentication scheme among 3 schemes and was given time to master the entry of the correct password for the chosen scheme. This was judged by successful input three times consecutively.

(d) The observers then returned to the inputter, and the inputter was asked to achieve 3 consecutive successful logins in the presence of the two observers. Mistakes by the inputter were ignored and the observers were able to take up any position around the inputter.

(e) The observers then were given a 30 second distractor task (reading a short text). After the distractor task, the observers attempted to input passwords that they had seen (Step (f)). A distractor task is common in memory studies, often in lieu of a lengthy delay between observation and recall [15][16]. In this paper, the use of a distractor task was motivated by our assumption that an observer cannot immediately make use of observed information. Actually, observers should remember the information over an extended time period and do something else, before they can commence an attack.

(f) Each observer had three attempts to input the passwords observed. If successful in less than three attempts, they were not required to login again using that scheme.

(g) Step (c)-(f) were repeated for each of the all schemes.

4.3 Result

1. Input time

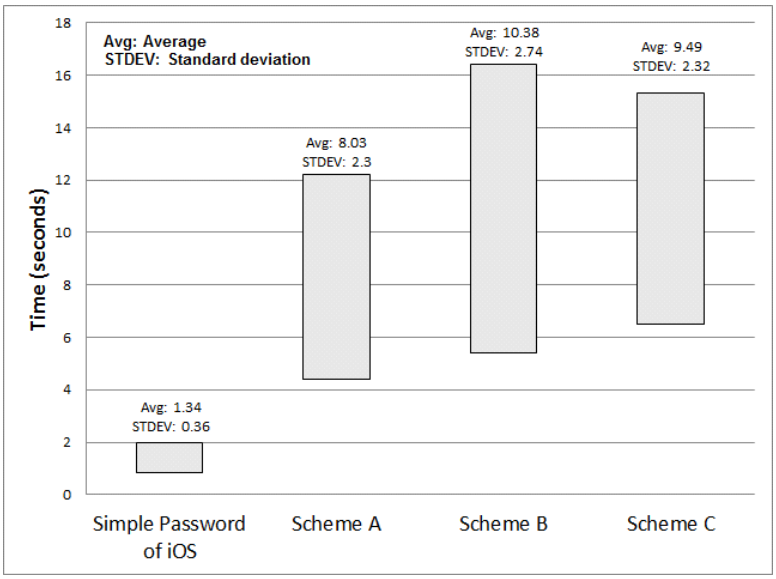

Figure 4.1: The Distribution of Successful Login Durations of Inputters

All participants showed very short duration for inputting passwords in 'Simple password' scheme

of iOS, since this scheme is very similar to PIN.

In Scheme A, the users spent about 10 seconds at the first attempt to input the password, and the last two attempts showed the tendency to input the password faster. Some participants could input the password faster than the former attempts since they had the combinations for four symbols for each digit of the password in mind. However, the weak point in which the combinations were too easy to be attacked appeared.

In Scheme B, the input time varies according to the combination of the password. For example, the password, like 3214, of which each digit has a small change, requires the very short input time, and the password, like 1728, of which each digit has a bigger change and which consists of numbers and characters, requires relatively longer input time.

In Scheme C, the input time varied according to the arrangement of the numbers of the scheme. If some numbers for the password are arranged in a group, the input time is relatively short, but if the numbers for the password are scattered in the arrangement, since the user spends more time to memorize the location of the numbers than the former situation, the input time is relatively long.

2. Input accuracy

   First, in Scheme B, there was no wrong input of the password. However, there were some wrong input in Scheme A and C.

   In Scheme A, there were 3 wrong inputs. A wrong input happened by pressing wrong the number button, and other two wrong inputs happened by being confused about the symbols.

   In Scheme C, there were 3 wrong inputs. The wrong inputs resulted from forgetting or mistaking the arrangement of the numbers.

3. Imitability

   In PIN, 19 of the 20 observers (95%) were able to replicate the passwords of the inputters. Since the inputters submitted their password 3 times and the observers were able to take up any position around the inputters, most of the observers were successful in observing the passwords. Most observed the pattern of finger-moving. In the first attempt of the inputter, they memorized the finger-moving of the inputter and in next two attempts, memorized the numbers pressed by the

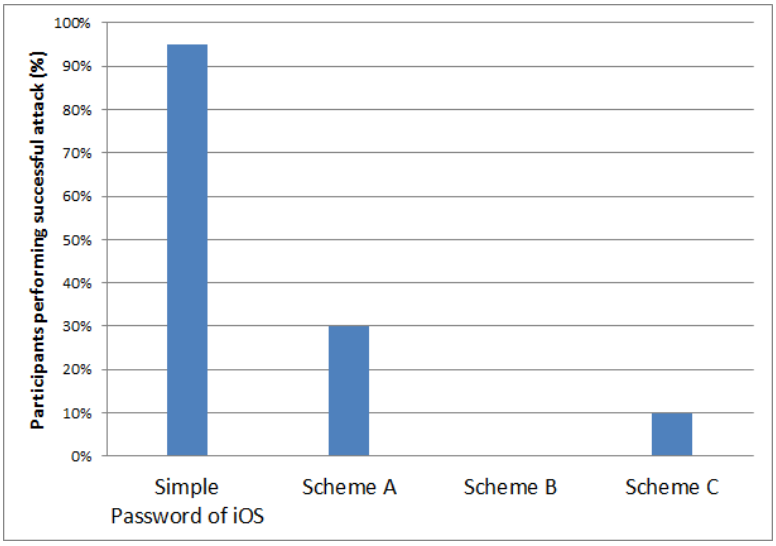

Figure 4.2: Percentages of Observers Able to Replicate the Password

finger.

In Scheme A, 6 of the 20 observers (30%) were able to replicate the passwords. Most of the observers who were successful in memorizing the passwords of the inputters aimed the moment when the inputter pressed just one button.

In Scheme B, all observers failed to observe the passwords. Some observers were able to detect one or two characters of the password when the shield gesture of the inputter was removed slightly from the screen. However, at the time, in order to see the part under the shield gesture, the observer moved her/his head close to the plane on which the device was.

The passwords in Scheme C were successfully observed by 2 of the 20 observers (10%). The inputters memorize only the locations of 4 or lower than 4 digits, but the observers memorize the locations of 12 digits. Also, the observers distinguish the tilt of the device.

4. Response of participants

After the experiment, all participants were asked to take part in a short questionnaire. 23 of the 30 participants (76.7%) were concerned about the ease of observing passwords and PINs entry (9 participants answered that they are always concerned, and 14 participants answered that they are concerned when they use the bank or stock applications.). All participants replied that Scheme B is the safest password scheme, and the 24 participants replied that if their own devices support

Scheme B, they will use the scheme in public environments.

About Scheme A, most of participants answered that Scheme A can be easy to the participants who are undergraduate or graduate students, but can be difficult to use to ordinary people.

About Scheme B, some participants replied that the scheme needs a wider screen. The iPad is sufficient for Scheme B, but in the iPhone, the wider screen is better than the present screen. Also, a participant answered that when moving, the input process in Scheme B is more difficult.

About Scheme C, some participants felt some pressure to memorize the location of numbers. Like Scheme B, there is a participant who answered that when moving, the input process in Scheme C is more difficult than on the table.

4.4 Discussion

To resist against shoulder-surfing attack, a strong point in Scheme A is that the observers are not able to know the meaning of the symbols right away. The second one is that the observers must memorize the number(s) with the symbols. The observers have to memorize at least two inputs per one-digit of the password. The third is that, all the time, the users are able to input the password in different ways.

However, the participants pointed out the weakness of Scheme A. First, there can be a person who is difficult to input the password with Scheme A. In the training session, some participants replied that Scheme A is difficult to input the password, although their input time is shorter than other proposed scheme. The second weakness is the simplification of the pattern of the input. Some inputters often input 1 with the 'Multiply' symbol and 0 with the 'Plus' symbol. Also, some participoants replied that 'Normal' and 'Ignore' symbols are not needed. They recommend other symbols like 'Square' and 'Minus'.

All participants replied that Scheme B can be resistant to shoulder-surfing attacks, too. Actually, all observers failed to observe the passwords.

The strong points of Scheme B are ease of input and small area under the shield gesture. Scheme B shows weakness in the input time, but most of the participants replied that the input time of Scheme B is endurable. However, some participants replied that in iPhone, the screen is small to use Scheme B, and Scheme B should be difficult to use when moving.

Some participants identified it as the strong point of Scheme C for the observers to memorize both

the locations of the numbers and the tilt information of the device. In the experiment, in fact, most of the observers replied that they were difficult to memorize both the locations and the tilt information.

However, some participants said that Scheme C could be attacked by the intersection attack. They replied that if they were able to observe with the record, they could know the password with the collected information. Also, in iPad, because of the big screen of the iPad, Scheme C is difficult to input the password. Finally, if the longer passwords are used, there is a weakness in which the users, also, memorize more locations of the numbers than the case of shorter passwords.

Except Scheme B, other both scheme A and C still are vulnerable to the attack with recording (replay attack). This means that 'Reduce visibility' is the most secure technique in the shoulder-surfing resistance techniques. Also, there is the weakness of the user friendliness. Long password input time makes users inconvenient. Poor usability within this context can lead to either: sloppy adherence to secure scheme on the part of the user (*e.g.* choosing easy passwords, taking notes, *etc.*), or users not using such scheme at all. Then, it needs the high resistance to shoulder-surfing and high user friendly password scheme.

Chapter 5. Conclusion

A smartphone is considered to a kind of a high-end mobile phone which has functions of contemporary feature phones and computers, with more advanced computing ability and connectivity. The number of the smartphone users in the world has been growing dramatically, and most of smartphones use Apple's iOS and Google's Android as their operating system. Also, after releasing iPad by Apple, the number of a tablet computer which looks like a small-sized computer is rapidly increasing. Since smartphones and tablet computers have functions of contemporary feature phones and computers, the security of smartphones and tablet computers must be more important than the general mobile phones and the traditional computers. Most of smartphones and tablet computers on the market currently support a full-touch screen for functions of computers. However, because of full-touch screens, smartphones have wider screens and keyboard than feature phones. Then, with these features, smartphones are vulnerable to the shoulder surfing.

In this thesis, we propose three new schemes: the multi-finger PIN pad (Scheme A), the password scheme with the wheels and the shield gesture (Scheme B), and the password scheme using tilt of the devices (Scheme C); and evaluate them. Our proposed methods hamper the observers who want to know the passwords of the users, using 'reduce visibility', 'subdivide action', 'dissipate attention', and 'knowledge transformation'. Comparing with existing password scheme, our methods are more resistant even though they have longer password input time. 95% of observers can replicate the passwords of PIN, but 30% of observers in Scheme A, 0% of observers in Scheme B and 10% of observers in Scheme C can replicate the passwords. We expect that our schemes can lead the users of smart devices to more secure use of them.

Summary

A Study on Shoulder-Surfing Resistant Password Scheme for Smart Devices with Full-touch Screen

스마트폰은 컴퓨터와 휴대 전화의 기능을 모두 가지고 있는 고급 기능의 휴대 전화이다. 전세계적으로 스마트폰의 사용자 수는 많이 늘어나고 있으며 스마트폰 대부분은 운영체제로 애플의 iOS와 구글의 안드로이드를 사용하고 있다. 또한, 애플의 아이패드가 발매한 이후, 태블릿 컴퓨터의 사용자 수 또한 많이 늘어나고 있다. 태블릿 컴퓨터 또한 스마트폰과 같이 대부분이 운영체제로 iOS와 안드로이드를 사용하고 있다. 스마트폰과 태블릿 컴퓨터 (이하 스마트 기기)는 컴퓨터와 휴대 전화의 기능을 모두 가지고 있기 때문에 보안이 그만큼 중요하다. 특히 풀 터치 스크린을 사용하면서 키보드가 따로 없이 스크린에 통합되어 있고, 크기가 커진 스크린은 어깨 너머 공격 (Shoulder Surfing)에 약점을 드러낸다. 이로 인해 많은 사용자들이 스마트 기기에서 패스워드를 입력하면서 불안해 하고 있다.

본 논문에서는 스마트 기기가 사용하는 풀 터치 스크린 환경에서의 어깨 너머 공격에 대응하면서 기존 스마트 기기의 단점들을 해결한 세 가지 암호 입력 방식을 제안하였다. 첫 번째 스킴 (Scheme A)은 숫자들과 간단한 연산 기호를 사용하여, 두 개 이상의 손가락을 통해 패스워드를 입력하는 방법, 두 번째 스킴 (Scheme B)은 가리는 동작과 함께 휠을 돌려서 패스워드를 입력하는 방법, 세 번째 스킴 (Scheme C)은 스마트 기기의 자이로스코프 센서를 이용하여, 무작위의 숫자의 배열을 보고 기기를 기울여서 패스워드를 입력하는 방법이다. 직접 사용자들이 참여를 하는 실험을 통하여 각 스킴의 어깨 너머 공격에 대한 대응성과 사용자 편의성을 검증하였다. 비록 입력 시간이 길다는 약점을 보였지만, 현재 스마트 기기에서 사용되는 패스워드 입력 방식에 대비해 뛰어난 어깨 너머 공격 저항성을 보였다. 특히 Scheme C는 모든 관찰자들이 패스워드 관찰에 실패하는 모습을 보였다. 우리는 제안한 스킴들을 통하여 스마트 기기 사용자들이 더욱 안전한 패스워드 입력을 할 수 있을 것이라 기대한다.

References

[1] C. Petty and H. Stevens, *"Gartner Says 428 Million Mobile Communication Devices Sold Worldwide in First Quarter 2011, a 19 Percent Increase Year-on-Year"*, Available: http://www.gartner.com/it/page.jsp?id=1689814

[2] T. Mainelli, J. Song, L. Loverde, and M. Shirer, *"Media Tablet and eReader Markets Beat Second Quarter Targets, Forecast Increased for 2011, According to IDC"*, Available: http://www.idc.com/getdoc.jsp?containerId=prUS23034011

[3] Editors PC Magazine, "Definition of: tablet computer". PC Magazine. April 17, 2010.

[4] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, *"Reducing shoulder-surfing by using gaze-based password entry"*, SOUPS. ACM, 2007.

[5] H. Gao, Z. Ren, X. Chang, X. Liu, and U. Aickelin, *"A New Graphical Password Scheme Resistant to Shoulder-Surfing"*, 2010 International Confer-ence on CyberWorlds, Singapore, 2010.

[6] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, *"Design and evaluation of a shoulder-surfing resistant graphical password scheme"*, AVI '06: Proceedings of the working conference on Advanced visual interfaces, pages 177–184, New York, NY, USA, 2006.

[7] C. Jones, S. Sinofsky, A. Leblond, M. Angiulo, and J. Larson-Green, *"Windows 8 Keynote #1"*, Available: http://channel9.msdn.com/events/BUILD/BUILD2011/KEY-0001

[8] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. Nicholson, J. Nicholson, and P. Olivier, *"Multi-touch authentication on tabletops"*, CHI '10: Proceedings of the 28th international conference on Human factors in computing systems, pages 1093–1102, New York, NY, USA, 2010.

[9] J. Marshall, T. Pridmore, M. Pound, S. Benford, and B. Koleva, *"Pressing the flesh: Sensing multiple touch and finger pressure on arbitrary surfaces"*, Pervasive Computing, Lecture Notes in Computer Science, pages 38–55. Springer, May 2008.

[10] K. Chalkias, A. Alexiadis, and G. Stephanides, *"A Multi-Grid Graphical Password Scheme"*, 7th Artificial Intelligence and Digital Communications conference (AIDC), 2006.

[11] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, *" The design and analysis of graphical passwords"*, SSYM'99: Proceedings of the 8th conference on USENIX Security Symposium, pages 1–1, Berkeley, CA, USA, 1999.

[12] D. Nali and J. Thorpe, *"Analysing user choice in graphical passwords"*, Tech. Report TR-04-01, School of Computer Science, Carleton University, Canada, 2004.

[13] J. Goldberg, J. Hagman, and V. Sazawal, *"Doodling our way for better authentication"*, CHI '02 extended abstracts on Human Factors in Computer Systems, 2002.

[14] F. Tari, A. A. Ozok, and S. H. Holden, *"A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords"*, SOUPS '06: Proceedings of the second symposium on Usable privacy and security, pages 56–66, New York, NY, USA, 2006.

[15] L. Koppenaal and M. Glanzer, *"An examination of the continuous distractor task and the long-term recency effect"*, Memory & Cognition, 18, 183-195, 1990.

[16] E. J. Davelaar, Y. Goshen-Gottstein, H. J. Haarmann, M. Usher, *"The demise of short-term memory revisited: empirical and computational investigation of recency effects"*, Psychological Review 112 (1): 3–42, 2005.

[17] D. Klein, *"Foiling the Cracker: a survey of, and improvements to, password security"*, 2nd USENIX Security Workshop, 5-14, 1990.

[18] E. Spafford, *"Crisis and aftermath (The internet work)"*, Communcations of the ACM 32(6), 678-687, 1989.

[19] E. Spafford, *"OPUS: Preventing Weak Password Choices"*, Computer Security. 11, 3, 273-278, 1992.

[20] D. Baker, *"Nondisclosing password entry system"*, U.S. Patent 5,428,349 June 27, 1995.

[21] A. De Luca, E. von Zezschwitz, and H. Hussmann, *"Vibrapass - secure authentication based on shared lies"*, 27th ACM SIGCHI Conference on Human Factors in Computing Systems. ACM, Apr. 2009.

[22] V. Roth, K. Richter, and R. Freidinger, *"A pin-entry method resilient against shoulder surfing"*, CCS '04: Proceedings of the 11th ACM conference on Computer and communications security, pages 236–245, New York, NY, USA, 2004. ACM.

[23] D. S. Tan, P. Keyani, and M. Czerwinski, *"Spy-resistant keyboard: more secure password entry on public touch screen displays"*, OZCHI '05: Proceedings of the 17th Australia conference on Computer-Human Interaction, pages 1–10, Narrabundah, Australia, Australia, 2005. Computer-Human Interaction Special Interest Group (CHISIG) of Australia.

[24] S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget, *"Design and evaluation of a shoulder-surfing resistant graphical password scheme"*, AVI '06: Proceedings of the working conference on Advanced visual interfaces, pages 177–184, New York, NY, USA, 2006. ACM.

Acknowledgement

이 논문을 완성하기까지 주위의 많은 분들께 도움을 받았습니다. 도움을 주신 모든 분들께 감사 드립니다. 김광조 교수님께서는 틈틈이 연구 상황을 확인해 주셔서 체계적인 연구방향을 세울 수 있었습니다. 그리고 연구실 선후배님 (규석이형, 장성이형, 진이형, 현록이형, Duc, Divyan, 혜란누나, 혜원이누나, Made, 도영이형) 들에게 연구실 생활 및 연구 등 많은 부분에서 격려 및 도움을 받았습니다. 모두들에게 고맙습니다. 또한, 바쁘신 와중에 학위논문심사를 위해 참석하셔서 진심 어린 조언을 주신 박진아 교수님과 이기혁 교수님께도 감사 드립니다.

부모님께 감사 드립니다. 사랑으로 저를 키워주신 덕분에 오늘의 제가 있을 수 있었습니다. 멀리서 나라를 지키면서 응원해준 동생과, 언제나 제게 힘을 주신 친척 모든 분께도 감사 드립니다.

실험에 참여해주신 모든 분들께도 감사 드립니다. 특히 의욕적으로 많은 도움을 준 민영이, 건하, 준수, 동우, 현일이, 민규에게 감사의 말을 전합니다. 이외에 제가 미처 언급하지 못한 고마운 분들이 너무나 많습니다. 저의 이 작은 결실이 도움을 주신 모든 분들께 조금이나마 보답이 되기를 바랍니다.

마지막으로 언제나 저를 올바른 길로 인도하시는 주님 감사합니다.

이 력 서

이 름 : 박 이 재

생 년 월 일 : 1988년 9월 1일

주 소 : 경기도 안산시 단원구 고잔2동 주공아파트 904동 1501호

E-mail 주 소 : krad@kaist.ac.kr

학 력

2004. 3. – 2006. 2. 경기과학고등학교

2006. 2. – 2010. 2. 한국과학기술원 정보통신공학과 (B.S.)

2010. 2. – 2012. 2. 한국과학기술원 전산학과 (M.S.)

경 력

2008. 2. – 2011. 12. 한국과학기술원 문지캠퍼스 도서관 사서

2011. 2. – 2011. 5. Introduction to Information Security, Undergraduate Teaching Assistant, KAIST

2011. 2. – 2011. 12. Introduction to programming, Undergraduate Teaching Assistant, KAIST

연 구 업 적

1. **Yi Jae Park**, Doyoung Chung, Made Harta Dwijaksara, Jangseong Kim and Kwangjo Kim, "An Enhanced Security Policy Framework for Android", 2011 Symposium on Cryptography and Information Security (SCIS 2011), Jan. 25-28, 2011, Kokura, Japan.
2. Doyoung Chung, Made Harta Dwijaksara, **Yi Jae Park**, Jangseong Kim and Kwangjo Kim, "An Efficient and Privacy Preserving Authentication Protocol for HAN", 2011 Symposium on Cryptography and Information Security (SCIS 2011), Jan. 25-28, 2011, Kokura, Japan.

3. Made Harta Dwijaksara, Doyoung Chung, **Yi Jae Park**, Jangseong Kim and Kwangjo Kim, "Secure, Fast Rebuilding and Energy Efficient Routing Protocol for Mission Critical Application over Wireless Sensor Networks", 2011 Symposium on Cryptography and Information Security (SCIS 2011), Jan. 25-28, 2011, Kokura, Japan.

4. 정도영, 김장성, Made Harta Dwijaksara, **박이재**, 김광조, "스마트 그리드에서의 전기자동차 충전을 위한 안전한 인증 및 과금결제 프로토콜", CISC-S'11 (2011년도 한국정보보호학회 하계학술대회) Proceedings, pp.221-226, 2011.6.24, 충남대학교, 대전. – 우수논문상

5. **Yi Jae Park**, Doyoung Chung, Made Harta Dwijaksara, Jangseong Kim and Kwangjo Kim, "An Enhanced Security Policy Framework for Android", Program of Triangle Symposium on Advanced ICT 2011 (TriSAI 2011), Aug. 25-26, 2011, KAIST, Korea.