Recent Emerging Security Threats and Countermeasure Concepts in Mobile User Authentication

Dongmin Choi[1] and Ilyong Chung[2*]
[1]Division of Undeclared Majors, Chosun University, Gwangju, Korea
jdmcc@chosun.ac.kr
[2]Department of Computer Engineering, Chosun University, Gwangju, Korea
iyc@chosun.ac.kr

Abstract

Over the past decades, mobile security threats have continued to change according to the mobile environment, which includes technical support such as mobile device specifications and network infrastructure. The current focus on security threats has not been on program defects in mobile devices but on errors made by human users (i.e., human or user errors). To prevent the damage from emerging threats, researchers have continued to propose alternative solutions. In this paper, we introduce several existing solutions corresponding to recent emerging security threats and briefly discuss the revealed problems and countermeasures.

Keywords: Mobile Security, Authentication, Graphical Password, Pattern Password, Keystroke Dynamics

1 Introduction

Our world is gradually transitioning into a society dependent upon mobile devices. Mobile devices are becoming common around the world. Users typically use mobile devices for their daily lives, such as for alarms, SMS, SNS, buying household goods, and banking services. Thus, users may be attracted to using mobile devices in their lives. In the future, mobile network will likely be easily accessible via WiFi or high-speed cellular networks and be available everywhere, even in remote, and hostile places. Thus, the number of users who access wireless networks to connect to Internet services will also sharply increase. With the advent of the mobile environment, privacy concerns will also increase significantly. As noted earlier, mobile devices are becoming closely related to human life. Moreover, based on their evolution, mobile devices will assist users throughout the users' lives. However, security and privacy problems become more important as devices become more closely connected to users because the information from a human can be considered biometric. In other words, it is unique information that can be used for user identification and authentication. According to the development history of recent security techniques for mobile devices, developers have recently been applying human biometric information to authenticate devices. Therefore, as compared to security techniques for desktop PCs, mobile-based security techniques have to diversely and deeply search for various possible ways of attack. In contrast to previous security threats that mainly relied on device or algorithmic error, recent emerging security threats have focused on the lack of human-side security awareness. Several mobile-based attacks may differ from the traditional attack pattern; one is human-error based attack. A representative attack technique that focuses on human error is the social engineering attack. Typically, users trust their own mobile device; this type of attack

IT CoNvergence PRActice (INPRA), volume: 4, number: 1 (March 2016), pp. 10-17
*Corresponding author: Department of Computer Engineering, Chosun University, Seoseok-dong, Dong-gu, Gwangju, 501759, Korea, TEL: +82-62-230-7712

technique exploits the trust relationship between man and machine. When the user operates a mobile device to run many kinds of tasks (e.g., mobile banking, commerce, login, or social network service), they typically input or send their secret information through the device without any doubt. However, during the interaction between man and machine, several weak points are revealed that can be exploited by an attacker. In this paper, we introduce some well-known emerging security threats for mobile devices and existing methodologies.

2 Recent Emerging Security Threats

As the number of mobile user increases, people may log into personal services with their private ID/-password at any time in any place via their mobile devices. However, emerging threats have focused on mobile devices and owner vulnerabilities. We categorize the vulnerabilities into two types:

1. Owner side: Human errors
2. Device side: screen size, touchable screen

On the owner side, human errors refer to problems caused by human mistakes. Typically, the owner uses a mobile device without being aware of the surrounding environment. Thus, the attacker may get a chance to obtain sensitive information. On the device side, mobile devices typically have LED or AMOLED screens of 4 or 5 in. These touchscreens also provide an input method to communicate with the owner. The owner inputs information via the touchscreen to communicate with the device. Most vulnerabilities are due to this process. Figure 1 shows the trend in the smartphone screen size over time.

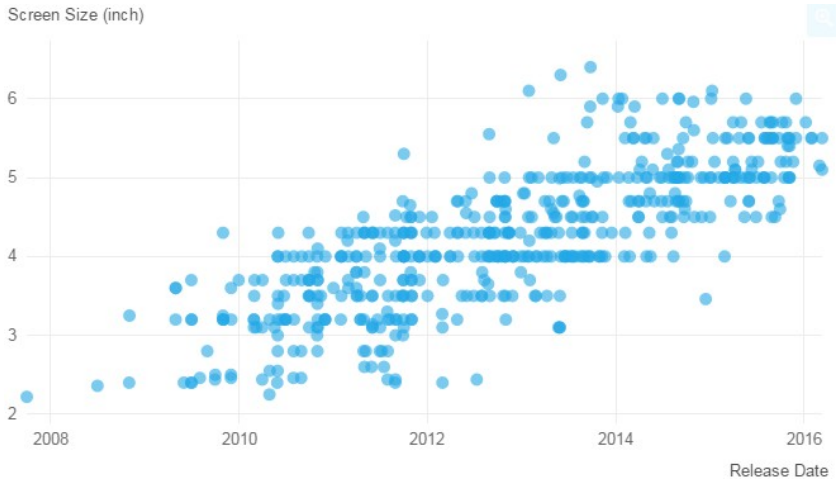

Figure 1: Smartphone screen size over time

Shoulder surfing As shown in Figure 2, shoulder surfing is an effective way to get information via direct observation by the attacker. The attacker looks over the user's shoulder to obtain secure information. Shoulder surfing can also be attempted at long distances with the aid of optical devices [9], [5], [12]. Particularly in crowded and public places, shoulder surfing is effective because of easier observation [14]. According to Honan [4], the results of a survey showed that 85% of non-authorized persons could see sensitive information on the screen of a mobile device. Moreover, 82% of users had little or no confidence in protecting their screen from being viewed by non-authorized people.

Recording The recording attack is similar to shoulder surfing. Some researchers have categorized recording as part of shoulder surfing because the technique is the same: the attacker observes the user to

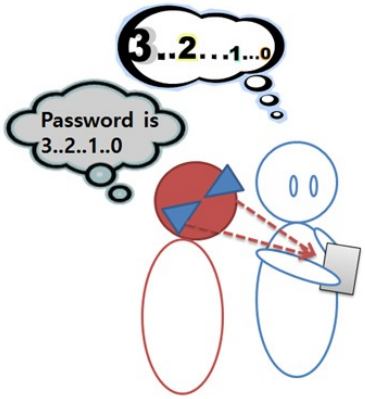

Figure 2: Shoulder surfing

obtain secret information via direct or non-direct optical devices, including the human eye. We divide these attacks according to the observation technique. With the recording attack, attackers do not use their eyes to get information but use optical or electronic recording devices. The range of available recording devices is not limited and can even exploit the embedded sensors in mobile devices.

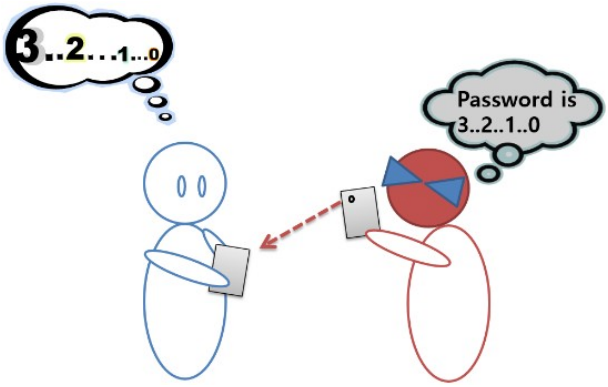

Figure 3: Recording

Smudge As shown in Figure 4, the smudge attack is a method of guessing and restoring the original password pattern from traces left on the touchscreen of a mobile device [15]. Typically, a user's finger leaves oily smudges after drawing the password pattern on the touchscreen. The smudge attack relies on oily smudges. After the finger smudges are detected, they can be directly used to unlock the device [1], [11].

Password guessing with embedded sensors Another type of network attack is password guessing [13], [2], [8]. Sensors embedded in the mobile device are used to achieve a higher attack success rate than the classical approach. When a user types a password with a virtual keypad or draw pattern, the values of the embedded sensors change continuously. Thus, by simulating the same device, the attacker guesses the appropriate key position or pattern shape to obtain secure information.

3 Existing Countermeasure Concepts

In order to ensure safety against the various attacks on mobile devices, researchers have recently proposed many concepts and mechanisms, as shown in Figure 5. However, compared to existing security

Figure 4: Smudge

Figure 5: Sensors embedded in a smartphone

mechanisms, several of these new mechanisms are still not suitable because of higher product cost. Thus, in this section we omit several high-cost mechanisms such as tokens, smartcards, and physical biometrics.

Graphical password Conventional password authentication methods mainly rely on the QWERTY keypad structure from the PC environment, which is transplanted into mobile devices regardless of the compatibility. Therefore, several problems occur in terms of the security and usability.

To cope with the attacks described in section 2, "what you know"-based graphical password input approaches have been proposed. With a graphical password, users do not need to remember text information and its sequence, even though the length of information is long [3].

Pattern password To cope with existing attacks, pattern-based authentication methods have been proposed. Nowadays, numerous modified versions have been developed with attractive benefits. Patterns are partially graphics-based, so they have similar advantages to graphical passwords. Android OS-based smartphones have pattern lock authentication, which is commonly used worldwide [7].

Keystroke dynamics This authentication mechanism verifies the user on the basis of the concept "keypad and keyboard typing patterns are different." In contrast to typical authentication mechanisms,

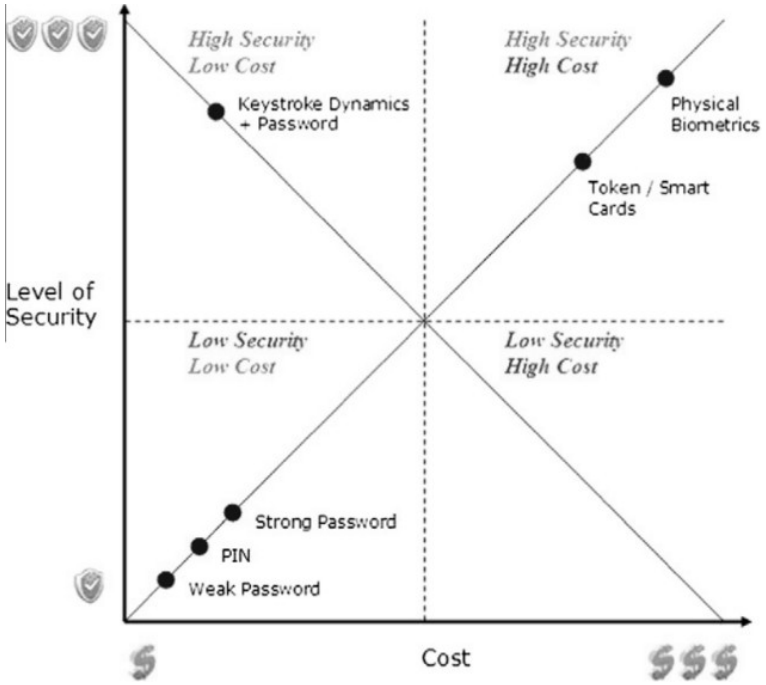

Figure 6: Comparison of security mechanisms in terms of security level and cost

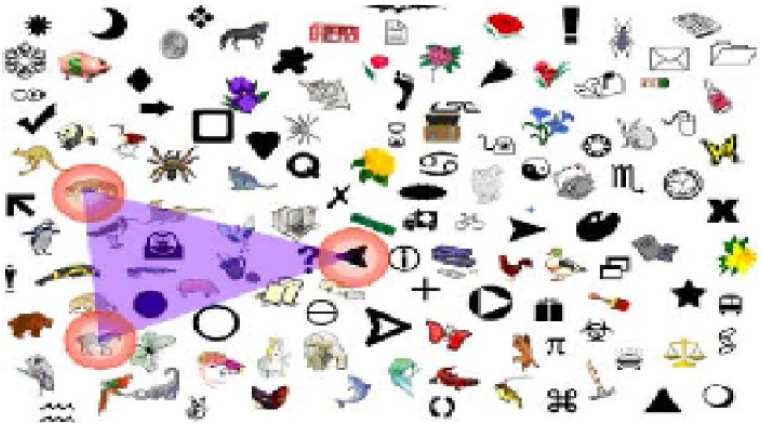

Figure 7: Example of graphical password scheme

the keystroke dynamics approach continuously checks and verifies the user in the background [6], [10]. For one-time authentication, the user registers a password pattern for algorithmic learning. Figure 9 shows the keystroke pattern differences. In the case of continuous user verification, sensors embedded in the mobile device continuously check and compare sensor data for verification against the data of the legitimate user.

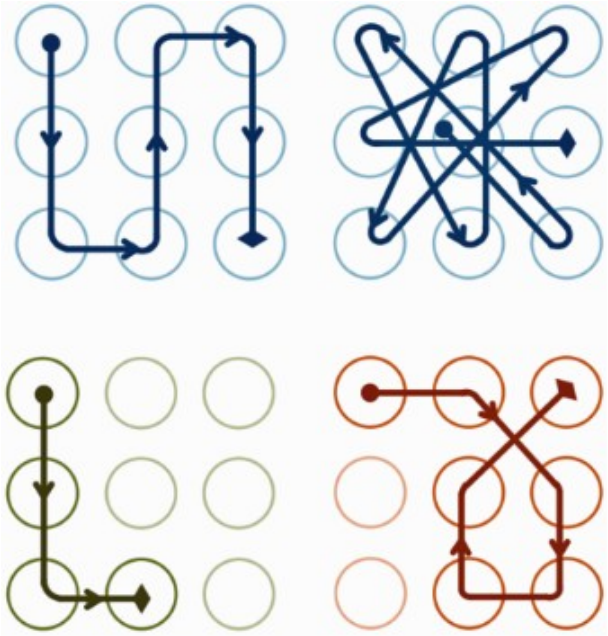

Figure 8: Example of pattern password

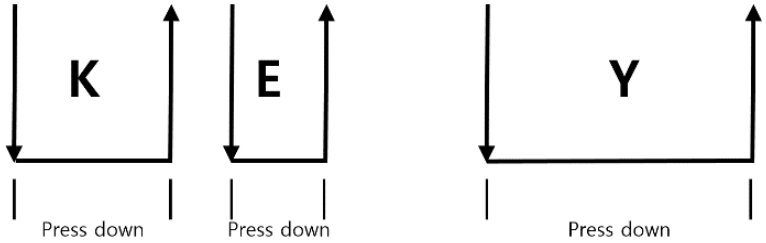

Figure 9: Keystroke pattern

4 Existing Problems and Suggestions

4.1 Graphical Password

Problems It is recommended to display no or less information to guide the user to input the password on the screen of the mobile device. In the case of a graphical password, it is not composed of text information, so the image and graphical components are easy to remember. However, this approach is still vulnerable to shoulder surfing, smudge, and password guessing with sensors. The reason is because graphical components are also easy for the attacker to remember. Thus, the attacker can easily obtain information by using electronic recording devices. Existing schemes mainly rely on displaying information to guide the user's password input.

Suggestions It is recommended to develop a nonvisible user graphical password authentication scheme. Typically, graphical components are visible. Thus, compared to text-based passwords, graphical passwords may be more vulnerable under specific conditions. The graphical password is assumed to use a user-predefined picture selection mechanism. In the case of a text-based password, a shoulder surfing attacker may find it difficult to guess the original password from a long distance. However, pictures are larger than text. Thus, a shoulder surfing attacker may be able to obtain a passcode from a long distance. Thus, one or two more authentication mechanisms need to be used in conjunction with a graphical

password.

4.2 Pattern Password

Problems The most well-known pattern password is pattern lock. However, pattern lock is vulnerable to shoulder surfing, smudge, and password guessing with sensors, including traditional password guessing attacks. Typically, pattern lock uses nine dots to link the line pattern. With nine dots, there is an insufficient number of cases for this approach to be robust against a password guessing attack. In addition, persons who use a pattern lock use simple patterns to unlock their phones.

Suggestions Nowadays, pattern information is visible in most cases. Thus, an invisible pattern password scheme needs to be developed. Pattern passwords that use sensors embedded in the mobile device are also a good way to develop an invisible scheme. To achieve a robust scheme against social engineering, two or three verification methods are also needed to authenticate the legitimate user.

4.3 Keystroke Dynamics

Problems With a recording attack, an attacker can easily obtain all of the keystroke information of a user. In the case of shoulder surfing, the attacker imitates the verified user's keystroke behavior. Keystroke actions are relatively easy to determine due to the rhythmical characteristics of the input action.

Suggestions The keystroke dynamics scheme is based on user behavior. Thus, the user's actions are easily exposed by shoulder surfing, smudge, and password guessing with sensors. Therefore, it is recommended to combine one or two more authentication schemes to verify the legitimate user and not use the keystroke scheme as the major authentication method for the combined schemes.

5 Conclusion

Graphics-, pattern-, and keystroke-based methods are not fully equipped to protect mobile users against social engineering attack scenarios. Mobile devices are personal and user-friendly; thus, they can contain significant personal information. Human errors are not deeply related security algorithm. Therefore, the owner can be susceptible to cybercrime when critical information is exposed by a human error, even if the mobile device itself is sufficiently robust against security attacks. Therefore, human characteristics need to be considered when developing robust mobile user authentication methods.

5.1 Future Work

To cope with the traditional, and upcoming security threats, we plan to further strengthen existing countermeasures. Moreover, we will categorize traditional, existing, and emerging security threats and countermeasures. After briefly discussing countermeasures against emerging attacks, we plan to propose several robust schemes against them.

References

[1] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith. Smudge attacks on smartphone touch screens. In *Proc. of the 4th USENIX Workshop on Offensive Technologies (WOOT'10), Washington, D.C., USA*, pages 1–7. USENIX, August 2010.

[2] L. Cai and H. Chen. Touchlogger: Inferring keystrokes on touch screen from smartphone motion. In *Proc. of the 6th USENIX conference on hot topics in security (HOTSEC'11), San Francisco, California, USA*, pages 1–6. USENIX, August 2011.

[3] P. Corporation. Passfaces: Two factors authentication for the enterprise. http://www.passfaces.com, 2005-2016.

[4] B. Honan. Visual Data Security White Paper. http://www.visualdatasecurity.eu/wp-content/uploads/2012/07/Visual-Data-Security-White-Paper.pdf, July 2012.

[5] H. Kim, H. Seo, Y. Lee, T. Park, and H. Kim. Implementation of secure virtual financial keypad for shoulder surfing attack. *Korea Institute of Information Security and Cryptography*, 23(6):21–29, December 2013.

[6] C. E. Larsen, R. Trip, and C. Johnson. Direct, Gesture-based Actions from Device's Lock Screen. US 8136053 B1, May 2016. http://www.google.com/patents/US8136053.

[7] J. B. Miller and J.-M. Trivi. Direct, Gesture-based Actions from Device's Lock Screen. US 8136053 B1, June 2011. http://www.google.com/patents/US8136053.

[8] E. Miluzzo, A. Varshavsky, and S. B. R. R. Choudhury. Tapprints: your finger taps have fingerprints. In *Proc. of the 10th international conference on Mobile systems, applications, and services (MOBISYS'12), Lake District, UK*, pages 323–336. ACM Press, June 2012.

[9] M. Rouse. Definition: Shoulder surfing. http://searchsecurity.techtarget.com/definition/shoulder-surfing, September 2005.

[10] D. Security. Keystroke Recognition. http://www.deepnetsecurity.com/authenticators/biometrics/typesense/, 2011.

[11] S. Shankland. 'Reverse smudge engineering' foils android unlock security. https://www.cnet.com/news/reverse-smudge-engineering-foils-android-unlock-security/, February 2012.

[12] H.-M. Sun, S.-T. Chen, J.-H. Yeh, and C.-Y. Cheng. A shoulder surfing resistant graphical authentication system. *IEEE Transactions on Dependable and Secure Computing*, PP(99):1–1, March 2016.

[13] J. Thomas. Password Guessing Attacks, Brute Force Attack, Dictionary Attack. http://www.omnisecu.com/security/password-guessing-attacks.php, May 2016.

[14] Wikipedia. Shoulder surfing (computer security). https://en.wikipedia.org/wiki/Shoulder_surfing, May 2016.

[15] Wikipedia. Smudge attack. https://en.wikipedia.org/wiki/Smudge_attack, May 2016.

Author Biography

Dongmin Choi received the B.E. degree in computer engineering from Kyunghee University, in 2003, and the M.S. and Ph.D. degrees in computer engineering from Chosun University, in 2007 and 2011, respectively. Since 2014, he has been a Professor with the College of General Education, Chosun University, Gwangju, South Korea. His research interests include information security, sensor network systems, mobile ad-hoc systems, smart grid home network systems, mobile sensor applications, and internet ethics.

Ilyong Chung received the B.E. degree from Hanyang University, Seoul, Korea, in 1983 and the M.S. and Ph.D. degrees in Computer Science from City University of New York, in 1987 and 1991, respectively. From 1991 to 1994, he was a senior technical staff of Electronic and Telecommunication Research Institute (ETRI), Dajeon, Korea. Since 1994, he has been a Professor in Department of Computer Science, Gwangju, Korea. His research interests are in computer networking, security systems and coding theory.