Press Code: A Shoulder Surfing Resistant Authentication Scheme for Smart Devices

Nur Nadiah Hanim Mohd Nor, M. S. A. Noman Ranak, Saiful Azad, Arafatur Rahman
Fakulti Sistem Komputer & Kejuruteraan Perisian, Universiti Malaysia
Pahang, Lebuhraya Tun Razak, 26300 Gambang, Pahang, MALAYSIA
nh.nadiahhanim@gmail.com, Sayfullahranak1993@gmail.com,
saifulazad@ump.edu.my, arafatur@ump.edu.my

Highlights: A memorization-based locking system is widely used in today's smart devices, where a user has to repeat a text/number/pattern/others from the remembrance that has been registered before. He/she would be allowed to access the device if the newly given password is matched with the registered one. However, among this class of passwords, graphical password schemes are more compatible for smart devices due to their heavily graphic-oriented nature. However, existing graphical password schemes experience various attacks and threats. Among them shoulder surfing is the most prominent one, where an attacker can observe the password through picking on the screen. In this project, we propose a shoulder surfing resistant password scheme using press code, which is a new kind of code; and hence, a novel authentication scheme. In the proposed technique, a user can authenticate thyself by repeating the registered press code. We implement our proposed technique on the Android platform, and we have a prototype to demonstrate at present.

Key words: *Smart devices, authentication, graphical password scheme, and press code.*

Introduction

Smart devices have been spread everywhere these days because of their special extra services, advanced technology and their functionalities compared to regular phones. For that reason, people store several private information, such as PIN numbers, essential documents, secret and public images, and other valuable data in their smart devices for frequent access. However, most people among them do not take even the basic steps to secure their smart devices. After a survey is conducted by Consumer Reports in USA, they discovered 39% of more than 100 million American adult smartphones owners failed to take even minimal security to protect their phone. However, there are a few users protect their phones, but only by using a basic screen-lock, 4-digit PIN to lock their phone (Jeffrey Fox, 2013).

Background and Motivation

The most commonly used authentication scheme in smart devices is text-based authentication, which is also known as alphanumeric authentication scheme. However, text-based scheme is vulnerable to password guessing attack, dictionary attack, shoulder surfing attack and also social engineering attack (Mokal P.H. and Devikar R.N., 2014). Moreover, the tiny screen size of the smart devices compels some constraints in text-based password scheme, e.g., limited length password, small on-screen keyboard. Due to the latter constraint, typing turn out to be less precise and inefficient. Consequently, people use even smaller passwords, which make them additionally vulnerable (Cooney, 2010). On the contrary, the graphical password scheme is more compatible for the smart devices due to their heavily graphic-oriented nature. In psychological studies, it has been observed that human can remember pictures better than text (R.N Shepard, 1967).

In addition, graphical password offers a larger space over text-based passwords and thus presumably offer better resistance to dictionary attack (Xiaoyuan Suo, Ying Zhu and G.Scott Owen., 2005). However, existing graphical password schemes are also vulnerable to various attacks and threats, namely shoulder surfing, smudge attack, brute force attack, intersection attack, reflection attack and so on (Arash Habibi, Samaneh Farmand, Dr. Omar and Dr.Rosli, 2009).

Most of the existing graphical password schemes fail to tackle aforementioned attacks. It still remains one significant research area to investigate and contribute. In this paper, we propose a new graphical password, which is capable of tackling shoulder surfing attack.

Proposed Scheme

In this section, the proposed authentication scheme is discussed in details at first. Afterwards, the configuration and authentication techniques using the Press Code are mentioned.

Press Code:

The force press (a.k.a., 3D display) is a new type of technique introduced to several recent smart devices. Due to its numerous usages, new smart devices are also incorporating this technique. In our proposed project, we utilize this technique to authenticate a user. There are manifold advantages of using this technique, i) no extra hardware is necessary if it is enabled in a smart device, ii) unlike other graphical password, it could be implemented even in small smart devices like smart watch, iii) no extensive training is necessary, and so on. In our proposed technique, we employ the existing force press of the smart devices to generate a code, called

Press Code (PC). In details, the presses of a user will be converted to a PC which will be stored in the device.
A user has to register a PC at the beginning of the authentication enabling process. Then, when the user wants to unlock the screen, he/she need to repeat code. The screen only will be unlocked if and only if the current PC is matched with the registered one.

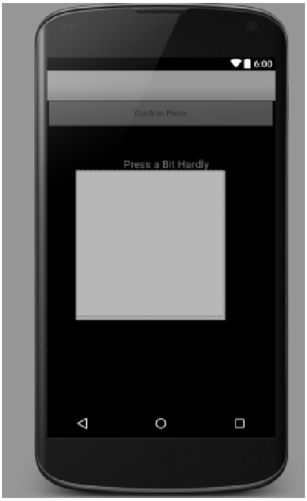

Figure 1: The grey, square area utilized in the proposed scheme is demonstrated on a smart phone screen.

In our proposed scheme, we only used a square area as depicted in Figure 1, where a user can commit presses; and hence, provide the PC. Within the area a user is free to provide press; on the contrary, the presses will not be counted. One advantage of using large area in our proposed scheme is that it can tackle the fat finger problem, which is common in smart devices. Thus, there is no problem for the people who have a bigger size of finger.

Configuration and Registration:

Before using our proposed scheme, a user has to launch the program and to register thyself by providing the PC. As mentioned before, a user can commit the press from any place within the square box. A user is independent to give any number of presses. The PC will be generated in two cases: i) after the user releases his or her finger from the screen; or ii) if the finger moves beyond the square box. The generated PC will be encrypted and then stored in the phone. It ended the registration process.

After completion of the registration procedure, the new authentication process is enabled. Every time when a user attempts to unlock the device, has to provide a new code. A user would be able to unlock the screen if and only if the newly given code is matched with the registered code.

Evaluation

In this subsection, the mechanisms that assist the proposed scheme to resist the considered attacks are discussed. For instance,

1) Dictionary Attack: Since the Press Code does not use any of characters or number, so it can prevent the dictionary attack.

2) Shoulder Surfing Attack: Since the Press Code is a touch-pressure technique, only the user who is pressing the screen by establishing his/her finger on the predefined area would be able to provide the code. Any attacker who is observing and/or capturing the screen unlocking session would not be able to discover it.

3) Smudge Attack: The proposed scheme is also resilient against the smudge attack; since, generally presses are concentrated within notable small area.

Other Aspects

Here, the other aspects of the proposed scheme, e.g., contribution to the society and advantages will be discussed in brief.

1) Contribution to the community: Currently, most of the people cannot think a day without smart devices. Password breaches to this kind of systems may harm to them. From a study, it has been found that overall financial losses due to compromised security increased 34% over the course of 2013, which is alarming (entrust, 2016). Consequently, a secure authentication scheme is necessary to resist password breaches. Our proposed scheme can resist three prominent attacks, namely shoulder surfing, smudge, and brute-force attacks.

2) Advantages: Our proposed scheme has manifold advantages:

- Ensures significant level of security by resisting prominent attacks
- No additional hardware is necessary to enable it in a smart device.
- Offers a large password space to the user.

3) Commercial value: If we consider the large smart phone market, the commercial value of this proposed scheme is huge, which could be more than several million dollars.

Conclusions

Existing graphical password schemes suffer from various attacks, such as shoulder surfing, smudge attack dictionary attack, and so forth. To offer protection against shoulder surfing, smudge, and dictionary attacks, we propose a new graphical authentication scheme, named Press Code (PC), where the force press of smart devices is converted to a code; and hence, the name. The proposed technique is implemented over Android platform, and currently, we have a working prototype. A survey has been conducted to find out the usability of the proposed technique; and users give positive replies.

Acknowledgement

This work has been partially supported by the RDU grant, RDU160353, of University Malaysia Pahang, Malaysia.

References

Jeffrey Fox (2013). 39 Percent of smart phone users don't secure their phones. Url: http://www.consumerreports.org/cro/news/2013/05/consumer-reports-39-percent-of-smart-phone-users-don-t-secure-their-phones/index.htm

Mokal P.H. & Devikar R.N. (2014) A Survey on Shoulder Surfing Resistant Text Based Graphical Password Schemes.
Url:
https://www.ijsr.net/archive/v3i4/MDIwMTMxNTkw.pdf

Cooney, M. (2010). 10 common mobile security problems to attack, PC World. Url: http://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html.

Xiaoyuan Suo, Ying Zhu & G.Scott Owen. (2005). Graphical Password: A Survey. Url: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1565273

R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 1967

Arash Habibi, Samaneh Farmand, Dr. Omar and Dr.Rosli, (2009). Shoulder Surfing Attack in Graphical Password Authentication. Url: https://arxiv.org/abs/0912.0951

Entrust. (2014). Data Breach Study Finds Breaches, Financial Losses on the Rise. Url: https://www.entrust.com/data-breach-study-finds-breaches-financial-losses-rise.