



VAP Code: A Secure Graphical Password Scheme for Smart Devices

Saiful Azad, M. S. A. Noman Ranak, Md Arafatur Rahman

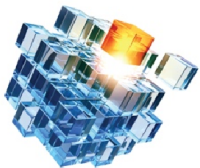
Fakulti Sistem Komputer & Kejuruteraan Perisian, Universiti Malaysia
Pahang, Lebuhraya Tun Razak, 26300 Gambang, Pahang, MALAYSIA
sayfullahranak1993@gmail.com, saifulazadump.edu.my,
arafatur@ump.edu.my

Highlights: In recent times when consumers around the globe are embracing smart devices at a higher ratio, they are also turning into a point of attraction to the attackers. As a result, a considerable amount of attacks is noted on these devices in the recent past. To combat with these attacks, many password-based authentication schemes are proposed. Among them, 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, e.g., shoulder surfing, smudge attack, intersection attack, reflection attack, brute force attack, and so on.

Key words: *Smart devices, authentication, graphical password scheme, vibration code, pattern lock, vibration and pattern code.*

Introduction

The smart devices could be considered as the modern-day's constant companion of the human being. For that reason, people store several private information, such as contact details, essential documents, secret and public images, PIN numbers, 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 conducted

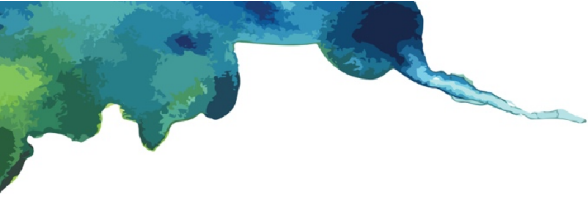


by the consumer reports in the USA, they discover that 34% of all smartphone owners do absolutely nothing, not even a simple code to lock the screen. On the other hand, only 36% of the smartphone users have set a basic 4-digit PIN to lock their phones (Weisbaum, 2014). This leaves the sensitive data stored on those devices unprotected.

Background and Motivation

The most common type of authentication scheme, which is utilized by many electronic devices is the text-based password. However, several cryptanalysts discovered various vulnerabilities of text-based password scheme, e.g., brute force attack, dictionary attack, social engineering attack, guessing attack, and so forth (Janczewski and Fu, 2010). 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 many psychological studies, it has been observed that human can recall visual images more effortlessly than text-based schemes. Therefore, it is less likely to be written down (Monrose and Reiter, 2005). Moreover, graphical passwords offer a larger symbol space over text-based passwords. Thereby, it is preferable in smart devices. 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 (Biddle, 2012).





Most of the existing graphical password schemes fail to tackle aforementioned attacks, which is detailed in Section II. Therefore, 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 three prominent attacks: shoulder surfing, smudge attack, and brute force attack.

Proposed Scheme

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

Vibration And Patter (VAP) Code:

The proposed graphical password scheme is comprised of two techniques: i) Vibration Code (VC) (a novel idea) and ii) Pattern Lock (PL) (modified from existing technique). Hence, it is named as Vibration And Pattern (VAP) code. Although, there are two separate techniques, but they coexist in such an inseparable way that to give a password no additional effort is necessary.

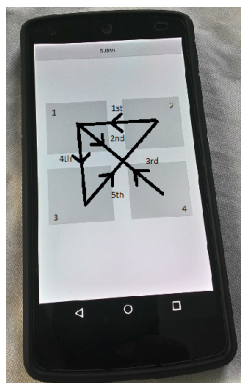
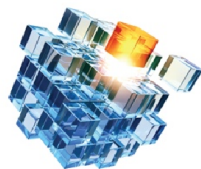


Figure 1: The 2×2 grid utilized in the proposed scheme is demonstrated on a smart phone screen

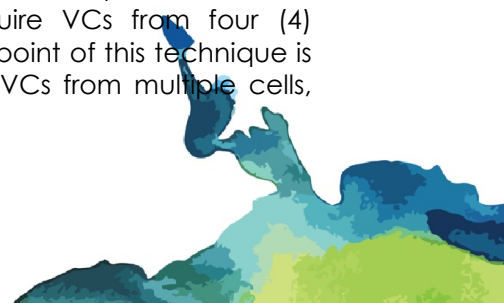


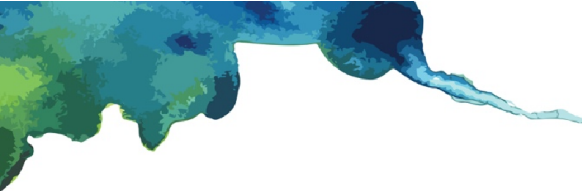
L	VAP Code			Android PL
	P_v	P_p	P	P
1	10	4	40	9
2	100	12	1200	56
3	1000	36	36000	320
4	10000	108	1080000	1624
5	100000	324	32400000	7152
6	1000000	1072	1072000000	26016
7	10000000	3216	32160000000	72912
8	100000000	9648	964800000000	140704
9	1000000000	28944	28944000000000	140704

Table 1: The password space of the proposed technique, which is compared with Android PL

Although, the vibration technique is currently available in most Android devices, we transform it to a new kind of code, named Vibration Code, which is compatible for the authentication process. A user has to register a VC at the beginning of the authentication enabling process. Next time, when that user endeavors to unlock the screen, he/she has to repeat the code. The user would be allowed to unlock the screen if and only if the acquired VC at the current session is equivalent to the one which is registered before.

In our proposed PL scheme, we make use of a 2×2 grid, i.e., four (4) cells. A cell in the grid could be considered as an area from where a user can acquire a VC. That means, a user can now acquire VCs from four (4) independent cells. A significant point of this technique is that when a user acquires the VCs from multiple cells,





he/she has already drawn a PL by connecting various cells. For instance, suppose a user has acquired VCs from the cells, such as {2, 1, 4, 1, 3, 2}. If we connect these cells, a PL is yielded as illustrated in Figure 1; and hence, the name.

Configuration and Registration:

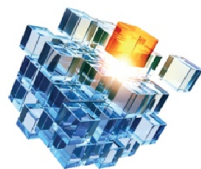
Prior using the proposed graphical password scheme, a user must register himself/herself to the system by providing a preferred VAP code. The user has the freedom to start sensing VC from any grid cell among the given four cells. The vibration starts when a user establishes his/her finger on a cell. After acquiring VC from that cell the user moves to the next cell and can continue until he is finished. Unlike Android, a user can visit the same cell multiple times. When a user moves his/her finger outside the grid area or release his/her finger, the system stops generating any vibration. This will be considered as the end of 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) Brute Force Attack: Since the VAP code is comprised of two separate techniques, it is essential to calculate the password space of the individual technique to find the final password space of the entire scheme. The password space is



shown in Table 1. As it could be observed that it offers a large password space over Android PL.

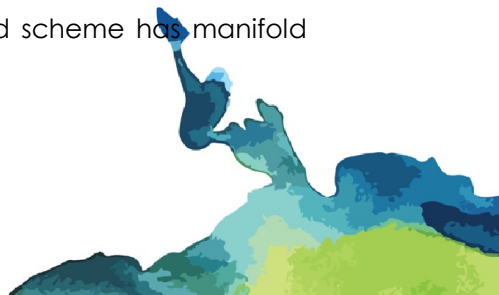
- 2) **Shoulder Surfing Attack:** Since the VC is a sense-based technique, only the user who is sensing the screen by establishing his/her finger on the predefined area would be able to acquire the code. Any attacker who is observing and/or capturing the screen unlocking session would not be able to discover it.
- 3) **Smudge Attack:** The proposed scheme is also resilient against the smudge attack even though smudges are generated when a pattern is drawn on the screen.

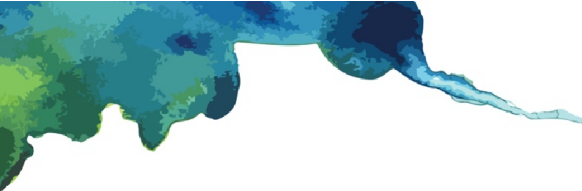
Thanks to the modified PL technique that permits a user to visit a cell multiple times. Consequently, it desponds all the endeavours of an attacker to extract the pattern.

Other Aspects

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

- 1) **Contribution to the community:** Currently, most of the people cannot think a day without smart devices. Password breach 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 percent over the course of 2013, which is alarming (entrust, 2016). Consequently, a secure authentication scheme is necessary to resist password braches. Our proposed scheme can resist three prominent attacks, namely shoulder surfing, smudge, and brute-force attacks.
- 2) **Advantages:** Our proposed scheme has manifold advantages:



- 
- i) Ensures significant level of security by resisting prominent attacks
 - ii) No additional hardware is necessary to enable it in a smart device.
 - iii) 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

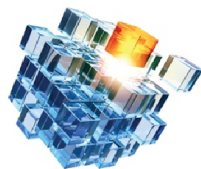
Existing graphical password schemes suffer from various attacks such as shoulder surfing, smudge attack brute force, intersection attack, reflection attack, and so forth. To offer protection against three prominent attacks, namely shoulder surfing, smudge attack, and brute force, we proposed a new graphical authentication scheme, named VAP code. It combines: i) the VC, where existing vibrations of the smart devices are transformed into a code; and ii) a modified PL technique. Both the techniques are blended in the system in a way that no additional effort is necessary to give a password. Moreover, no additional hardware is necessary to enable this scheme in existing smart devices.

Acknowledgement

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

References

- Weisbaum, H. (2014). Most Americans don't secure their smartphones. Url:
<http://www.cnbc.com/2014/04/26/most-americans-dont-secure-their-smartphones.html>.



- Janczewski, L. J., & Fu, L. (2010). Social Engineering-Based Attacks: Model and New Zealand Perspective. In Proc. of the International Multiconference on Computer Science and Information Technology. 847-853.
- 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>.
- Monrose, F., & Reiter, M. K. (2005). Graphical Passwords, in Security and Usability. L. Cranor and S. Garfinkel, Eds. Cambridge, MA: OReilly. ch. 9. 147-164.
- Biddle, R., Chiasson, S., & Oorschot P. C. V. (2012). Graphical Passwords: Learning from the First Twelve Years. ACM Computing Surveys. 44 (4).
- 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>.

