A Hybrid Screen Size Independent Authentication Scheme for Smart Devices

Ahmad Faizuwan Bin Welhendri1, Saiful Azad1,2,∗, Md Sayfullah Al Noman Ranak1
1Faculty of Computer Systems & Software Engineering, University Malaysia Pahang, 26300 Gambang, Kuantan, Pahang, Malaysia
2IBM CoE, UMP, 26300 Gambang, Kuantan, Pahang, Malaysia
E-mail: saifulazad@ump.edu.my (∗corresponding author)

August 2019

Abstract. Although, several authentication schemes have already been proposed for smart devices; however, most of these schemes does not consider the fact that smart devices come in different sizes. Hence, they are not screen size independent — which is the point of interest in this paper. Again, alongside screen size independence, a secure scheme also must defend the aforementioned attacks. Taking these concerns into account, in this paper, a hybrid screen size independent authentication scheme is proposed for smart devices that integrates Vibration Code or VC and Press Touch Code or PTC using a juggling-based approach. Here, VC ensures resilience against the shoulder surfing attack since it is a sense based technique and hybridization of both these schemes contribute to attenuating resilience against the smudge and brute force attacks up to some extent. In addition, the proposed scheme does not require a space more than the placement of a finger on the screen; and thus, it is screen size independent. The proposed scheme is evaluated in terms of security and functionality; and compared with other similar schemes where it outperforms the others.

Keywords: Graphical authentication, vibration code, press touch code, screen size independent scheme, hybrid authentication scheme.

1. Introduction

Due to offering an extensive variety of functionalities to users, smart devices are becoming a part of daily lives [1]. Therefore, for frequent access, many people prefer to store both sensitive and private data (e.g., passwords of other systems, sensitive documents, private images and so on) in these devices. However, due to lack of or insufficient protection, sometimes attackers capture these data and make them victimized. One of the easiest mechanism to protect contents in these devices is to utilize an access control mechanism. For that, authentication schemes are more preferred for these devices.

Till date, a considerable number of authentication schemes are already proposed. Most of these schemes could be broadly divided into three factors, namely i) knowledge or something
Hybrid Authentication

you know (e.g., PIN, textual password), ii) possession or something you have (e.g., token, smart card), and iii) inheritance or something you are (e.g., biometrics) [2]. Among them, knowledge-based schemes are utilized in most of the smart devices since they do not need any extra hardware (like inheritance) or any additional substance (like possession). Again, the knowledge-based schemes can be divided into several categories including textual schemes and graphical schemes. Among these categories, graphical schemes are more preferable to the general user due to their graphic oriented nature [3]. It has been established through several psychological studies that human brain can recall images more precisely than texts [4]. However, many of these schemes suffer from several attacks, such as smudge [5], shoulder surfing [6], and brute force [7] are the most prominent attacks. Over and above, most of these techniques are not screen size independent; whereas, screen of smart devices comes in different sizes. Due to this, sometimes it becomes difficult to provide credentials; specially on miniature smart devices. Therefore, in this paper, a hybrid scheme is proposed that is screen size independent and is resilient against the aforementioned three prominent attacks.

The subsequent sections of this paper are organized as follows. In Section 2, similar schemes are scrutinized to establish the necessity of proposing a new scheme. Afterwards, the proposed scheme is detailed in Section 3. Then, it is evaluated and compared with other similar schemes in Section 4. The concluding remarks of this paper and the future directions of this work are mentioned in Section 5.

2. Related Works

Since a specific scheme has specific defend mechanism that can tackle one or more attacks, a rational combination of two or more schemes would increase the level of security. In this case, two approaches are generally employed, namely i) multi-factor authentication and ii) hybrid authentication. In case of the former approach, as the name suggests, two or more factors (which are mentioned in Section 1, i.e., knowledge, possession, and inheritance) are combined to ensure higher level of security. A user would be granted access only after successfully presenting two or more pieces of evidences or factors. Conversely, in case of the latter approach, two or more schemes of a same factor are combined. In this paper, this approach is embraced since it takes considerably shorter time to authenticate over multi-factor approach. It is because, the selected schemes of a hybrid approach could be seamlessly combined, which is extremely unlikely in case of multi-factor approach.

At present, only a few hybrid authentication schemes are proposed. For instance, a such authentication scheme is proposed in [8], which utilizes a textual authentication scheme along with grid cells for generating credentials for Personal Digital Assistants (PDAs). However, it lacks adequate users’ study to endorse their claim of defending attacks like brute force, shoulder surfing, and dictionary. In [9], another hybrid authentication scheme is proposed that is based on shape and text. Here, the shapes of strokes are provided as the elementary part of the credential followed by the text. One of the primary concerns of this scheme is its registration process where a user has to mention the original shape and strokes to the system. Any attacker who is observing the registration session would be able to capture the
Hybrid Authentication

Figure 1. Raw data and Smoothed data for span = 3 are shown.

password. Again, because of the adaptability issue, usually users select considerably weak strokes, and thus, make this scheme vulnerable to several attacks. Again, another similar authentication scheme is proposed in [10] that combines image and text. The primary targets of this combination are to increase password space and memorability. However, this scheme is vulnerable to the shoulder surfing attack since both predecessors — image and text — are vulnerable to this attack. Therefore, designing a hybrid authentication scheme still remains an important issue to investigate.

3. Proposed Scheme

In this paper, a new hybrid authentication scheme is proposed that combines VC [11] and PTC [3] schemes. Here, the PTC is a special code, which is extracted from the pressure intensity values of a user and the VC is another special code, which is generated from the vibration. The justifications of combining these two schemes are that VC has the resilience against the shoulder surfing attack; however, it spends a long time during authentication. Conversely, PTC spends a short time for authentication; however, it experiences the shoulder surfing attack when attackers are relatively near. The details of these schemes and their combination mechanism are mentioned below.

3.1. PTC Scheme

The detail description of the PTC scheme is given in [3]. Therefore, a brief description is mentioned in this section for better understanding of the hybridization process. This scheme is based on the number of force presses provided by a user on a screen. For that, a Pressure Sensitive Screen (PSS) is obligatory, which can recognize the Press Intensity Value (PIV) at any certain time, \( \tau_i \). Generally, PIVs are recorded after every \( \delta \) time interval. However, in our proposed scheme, PIVs are acquired through a system call, which is performed after every \( \Delta \) time interval, where \( \Delta > \delta \). Every system call returns a PIV, \( \nu_i \) which is later saved in a list, \( \lambda \) chronologically, i.e., \( \nu_i \) is acquired before \( \nu_{i+1} \) and after \( \nu_{i-1} \). This way, the number of system calls as well as the number of PIVs in \( \lambda \) are reduced to facilitate data acquisition and data processing. This process starts with the placement of a finger on the screen and ends when the finger is taken off from the screen. In other words, data (i.e., PIV) acquisition starts
Hybrid Authentication

![Diagram of hybrid authentication scheme]

Figure 2. A high-level depiction of the proposed hybrid authentication scheme.

when a touched occur on the screen and ends when a detached occur from the screen.

After the completion of data acquisition phase, the subsequent phase is data cleaning. All the acquired data in $\lambda$ are cleaned using the Moving Average Filtering Technique (MAFT) technique [12]. The following equation is employed in this case:

$$
\nu'_i = \frac{1}{2N+1} \left( \nu_{(i+N)} + \nu_{(i+N-1)} + \ldots + \nu_{(i-N-1)} + \nu_{(i-N)} \right)
$$

(1)

where $\nu'_i$ is the PIV at $i$-th data point in $\lambda$ after the smoothing process, $N$ is the number of neighboring data points on either side of $\nu_i$, and $2N+1$ is the span. Among various spans like 3, 5, 7, 9, and others; span = 3 is selected taking the arguments in [3] into account. The justification of this choice is that higher span values flattens the peaks and hence, makes the presses undetected. Figure 1 demonstrates raw data and cleaned data for the span = 3.

Afterwards, the number of force presses is extracted from the cleaned PIVs in $\lambda$. As could be observed in Figure 1 is that force presses produce peaks. Therefore, a 1-D Peak finding algorithm [13] is modified in [3], called Press Touch Finding Algorithm (PTFA), which is also utilized in this paper for finding force presses or PTC. In brief, PTFA is a brute force based technique that selects a data point as a peak only if it is higher than its adjacent data points, and can be represented as below:

$$
\nu_{i-1} < \nu_i > \nu_{i+1}
$$

(2)
Hybrid Authentication

This equation identifies all local maximum peaks. The count of these local maximum peaks is the PTC. For instance, in Figure 1, PTC = 20 since there are 20 local maximum peaks. Afterwards, this value is either stored (in case of registration) or compared (in case of authentication).

3.2. VC Scheme

The detail description of the VC scheme is mentioned in [11]. However, for the better understanding of the proposed hybrid scheme, a brief description is given below. When a finger is placed on the screen, vibrations triggered with a specific time interval. It ends when the finger is lifted up from the screen alike the PTC. The number of vibrations that are sensed within this epoch is considered as the VC. Note that, for the VC scheme, vibrations need to be controlled (i.e., start, end, and interval between two vibrations) by the scheme. After the VC is counted, it is either stored for registration or compared for authentication.

3.3. Integration

For combining the aforementioned schemes, a juggle-based approach is considered, where the registration and/or the authentication commences with the VC, then the PTC, again the VC, and this sequence repeat until the session ending event occurs. Assuming every VC or PTC giving event as a cycle, the commencement of the next cycle must not exceed a fixed time, called interval threshold, $\tau_{max}$. Conversely, it is considered as the end of the registration or authentication session. In other words, after completion of a cycle, the next cycle must commence before interval threshold expired. In case of ending the session, a user must not place finger within $\tau_{max}$ on the screen. A high-level pictorial description of the proposed scheme is given in Figure 2.

3.4. Registration and authentication

At first, a user has to register a credential for enabling authentication-based access control on a smart device. For that, the user need to place a finger on the screen. As mentioned in Section 3.3, the first cycle of the scheme is the VC. Once the VC is provided, the user has to lift the finger. Afterwards, before $\tau_{max}$ expired, s/he has to place the finger on the screen and need to provide the PTC; and then, the VC. The user can juggle between the VC and the PTC as long as s/he wants. For higher level of security, the users are suggested to repeat the cycles for a considerable number of times (for more details, see Section 4.1.3). The user can end the session by not touching the screen before $\tau_{max}$ timer expired. At the end of the session, the credential of the user is stored in the system for utilizing in authentication.

After the completion of the registration, every time during the access to the device, the user has to recall the credential. The process of authentication is similar like the registration. However, at the end, instead of storing the credential, the newly provided credential will be compared with the registered credential. The user will be given access only if both the credential matched.
Hybrid Authentication

4. Evaluation

The proposed scheme is implemented on the Android Operating System and is tested on a Huawei P9 Plus device (which is a PST enabled device). The performance of this scheme is analyzed below in terms of security and functionality.

4.1. Security Analysis

For analysing the security of the proposed scheme, its resilience against three most prominent attacks, namely shoulder surfing, smudge, and brute force are taken into account.

4.1.1. Shoulder Surfing Attack: Since the VC is a sense-based scheme, it is resilient against the shoulder surfing attack as only a user who touched the screen would be able to sense the vibration. Any other who is picking on the phone or capturing the authentication session using a camera would not be able to acquire the credential. In addition, the PTC also offers resilience against this attack up to a certain extent as demonstrated in [3] with an experimental evaluation. According to that, it offers: negligible or no defence when the distance is near (< 0.5 m), seldom recognize from a mid range distance (2 to 3 m), and hard to recognize from a long range distance (> 3 m). Hence, the proposed technique inherits shoulder surfing resiliency from its predecessors.

4.1.2. Smudge Attack: This attack occurs when oily residues or smudges remain on the screen of a device as a side effect of proving a credential. In [5], it has been exhibited that around 92% cases, it is possible to break credentials partially and 68% cases fully. However, in the proposed scheme, it is not possible to find the VC and/or the PTC using the oily residues or smudges; and hence, it is resilience against this attack.

4.1.3. Brute Force Attack: An authentication scheme generally attains resilience against the brute force attack when it offers a large password space. Note that, in this attack, all possible combinations are checked systematically to break a credential. However, when the password space is large, it becomes infeasible. This proposed scheme offers a comparable password space like the Personal Identification Number (PIN). It can be calculated as $\gamma^\alpha$, where $\gamma$ is the maximum number of allowable VC or PTC in a cycle and $\alpha$ is the number of cycles. When $\gamma$ is 10 and $\alpha$ is 6, the password space of the proposed scheme is equivalent to a 6-digit PIN number, which is used in Automated Teller Machine (ATM) of banks in many countries and considered as a considerably strong password in terms of brute force attack when maximum three consecutive attempts are allowed within a certain time.

4.2. Functionality Evaluation:

This evaluation is most important since one of the objectives of this paper is to propose a screen size independent authentication scheme, which is a function of an authentication scheme.
Hybrid Authentication

Table 1. Comparison of the proposed technique with other similar techniques.
Here, attacks are typed in the italic font and functions are typed in typewriter font.

| Attack(s)/Function(s) | Vibration Code | Press Touch Code | Knock Code | Proposed technique |
|-----------------------|----------------|------------------|------------|-------------------|
| Shoulder Surfing       | H              | M                | M          | H                 |
| Smudge                | H              | H                | H          | H                 |
| Brute Force           | M              | M                | M          | M                 |
| Screensizeindependence | Y              | Y                | Y          | Y                 |
| Short Authentication Time | N          | Y                | Y          | Y                 |

Legends: L – Low, M – Medium, H – High, Y – Yes, N – No

4.2.1. Screen Size Independence Although, many authentication schemes are in operation at present; majority of them are not screen size independent. Hence, they are not appropriate for several smart devices, more specifically, for miniature devices where screen sizes are limited like smart watch, smart band and so on. For instance, most of the textual authentication schemes are not screen size independent since a full or partial keyboard will not fit in such devices. On the other hand, similar contention also could be raised for the graphical authentication schemes since they need a considerable screen size for displaying graphics. For the proposed scheme, a place for touching the screen is enough to provide both the VC and the PTC; and hence, it is a screen size independent authentication scheme.

4.2.2. Comparably low authentication time The proposed scheme spends relatively shorter registration or authentication time with respect to several similar techniques including VC and Vibration And Pattern (VAP) code [11]. Although, these schemes are resilient against the shoulder surfing and smudge attacks; its registration or authentication duration is relatively large. According to [3], between 4 to 10 seconds are spent for registration or authentication. Conversely, since the proposed scheme integrates the PTC which takes a shorter time for similar purposes; hence, the total duration would be reduced.

4.3. Comparison with other similar schemes

Among the existing authentication schemes, only a few can be considered as screen size independent authentication scheme, including VC, PTC, and Knock Code (KC) [14]. Their comparison with respect to security and functionality are mentioned in Table 1. As could be observed from the table is that PTC and KC are moderately resilient against the shoulder surfing attack; whereas, VC and the proposed technique offers the highest level of resistance against this attack. Again, all the compared schemes are highly resistant against the smudge attack and moderately resistant against the brute force attack.

In terms of functionality, all the proposed technique are screen size independent since they are chosen accordingly. Here, it is noteworthy to mention that all these compared schemes have variants that are not screen size independent. For instance, when these schemes are enhanced with grid cells, they are not screen size independent since a cell must be of a considerable size to provide VC or PTC or KC. Again, in case of short authentication time, all except VC spends a short duration for authentication. Generally, the VC takes a duration
Hybrid Authentication

between 4 to 10 seconds for authentication as mentioned earlier in Section 4.2.2.

From the above discussion, it can be observed that the proposed scheme offers either equal or more resilience against the attacks as well as the functionality. Therefore, we can conclude that the proposed scheme is superior over other similar schemes.

5. Conclusions & Future Works

In this paper, a new hybrid graphical authentication scheme is proposed that integrates both the VC and PTC using a juggling-based approach to ensure a high-level security in terms of attacks like shoulder surfing, smudge, and brute force until a certain extent. Moreover, the proposed scheme is screen size independent and can be implemented even in miniature smart devices including smart watch and smart band. The performance of the proposed scheme is compared with other similar screen size independent authentication schemes, and it is found that it performs superiorly over others.

In future, we would like to extend the proposed technique in a way that a user does not have to lift off the finger when one cycle is finished. For that, it is necessary to identify the switching conditions, i.e., when a user would like to provide the VC and when it is the PTC. Again, there would be no fixed scheme to start with. A user can start providing the PTC or the VC and then switched to the other.

Acknowledgement

This work has been partially supported by the RDU grant, RDU1703100, of University Malaysia Pahang, Malaysia.

Referencing

[1] Chang Y F, Chen C and Zhou H 2009 Computer Standards & Interfaces 31 740–747
[2] Gibson D 2011 Understanding the Three Factors of Authentication URL http://www. pearsonitcertification.com/articles/article.aspx?p=1718488
[3] Ranak M S, Azad S, Nor N H B M N and Zamli K Z 2017 PLoS ONE 12
[4] Adebola O, Ithnin N, jali M Z and Akosu N 2013 Journal of Theoretical and Applied Information Technology 53 124–130
[5] Aviv A J, Gibson K, Mossop E, Blaze M and Smith J M 2010 Smudge attacks on smartphone touch screens Proc. of 4th USENIX Workshop on Offensive Technologies
[6] Goucher W 2011 Computer Fraud & Security 2011 17–20
[7] Calculating password complexity URL https://thycotic.force.com/support/s/article/Calculating-Password-Complexity
[8] Sreelatha M, Shashi M, Anirudh M, Ahamer M and Kumar V M 2011 International Journal of Network Security & Its Applications 3 111–119
[9] Zhang Y, Monrose F and Reiter M K 2010 The security of modern password expiration: An algorithmic framework and empirical analysis Proc. of 17th ACM conference on Computer and communications security pp 176–186
[10] Mackie I and Yldrm M 2018 A novel hybrid password authentication scheme based on text and image Proc. of IFIP Annual Conference on Data and Applications Security and Privacy
Hybrid Authentication

[11] Azad S, Rahman M, Ranak M S A N, Ruhee B M F K, Nisa N N, Kabir N et al. 2017 Computers & Electrical Engineering 59 99–110
[12] Ahmed N and Rao K 2012 Orthogonal transforms for digital signal processing 1st ed vol 1 (Springer Science & Business Media) ISBN 9783642454523
[13] Cormen T H 2009 Introduction to algorithms (MIT press)
[14] LG Corporation Korean Patent 10-1404234, 2014 Knock code