The Coin Passcode: A Shoulder-Surfing Proof Graphical Password Authentication Model for Mobile Devices

The Next Generation Swift and Secured Mobile Passcode Authenticator

Teoh joo Fong[1], Azween Abdullah[2], NZ Jhanjhi[3]
School of Computing & IT (SoCIT),
Taylor's University,
Subang Jaya, Selangor, Malaysia

Mahadevan Supramaniam[4]
Research & Innovation Management Centre,
SEGI University,
Malaysia

***Abstract*—Swiftness, simplicity, and security is crucial for mobile device authentication. Currently, most mobile devices are protected by a six pin numerical passcode authentication layer which is extremely vulnerable to Shoulder-Surfing attacks and Spyware attacks. This paper proposes a multi-elemental graphical password authentication model for mobile devices that are resistant to shoulder surfing attacks and spyware attacks. The proposed Coin Passcode model simplifies the complex user interface issues that previous graphical password models have, which work as a swift passcode security mechanism for mobile devices. The Coin Passcode model also has a high memorability rate compared to the existing numerical and alphanumerical passwords, as psychology studies suggest that human are better at remembering graphics than words. The results shows that the Coin Passcode is able to overcome the current shoulder-surfing and spyware attack vulnerability that existing mobile application numerical passcode authentication layers suffer from.**

Keywords*—Mobile graphical password; multi-elemental passcode; shoulder-surfing proof passcode; mobile authentication model

I. Introduction

Authentication technology is crucial to the integrity and confidentiality of smart mobile device users, especially when many important features such as banking and finance are easily accessible through mobile applications. Current mobile security mechanisms use the four or six pin numerical passcodes which are easily remembered, while providing a swift security authentication for the users.

However, this security mechanism has its flaws when it faces modern attackers who can easily guess or shoulder surf for the password combinations. There are several other user authentication mechanisms such as the alpha-numerical passwords and the pattern drawing lock, which are also prone to shoulder surfing attacks. The two-factor authentication can be easily compromised when the first level protection of the mobile devices is vulnerable.

The Coin Passcode Graphical Password Authentication mechanism is a concept of the Cognitive biometric authentication which uses the hybrid scheme graphical password authentication mechanism. This paper is structured in six sections, including the Introduction Section, Related Works, The Coin Passcode Mobile Graphic Authentication Model, Security Analysis and Usability Metrics, Discussion and Conclusion.

II. Related Works

The related works of other existing and researched graphical password authentication model are discussed under this chapter.

A. Cognitive Biometrics

There are several different biometric authentication types including physiological biometrics and cognitive biometrics authentication. Under the Cognitive biometric authentication methods [1], user behaviors are identified using mobile phone sensors, through activities such as gestures and walking patterns. The input patterns are used as a means of behavior authentication. Several researchers have [2] analyzed the key input mechanics and patterns used by the users when they press the on-screen buttons to type on the phone.

Another research conducted by Giuffrida [3], allows Cognitive Authentication when the user types the password, where the movement and touch of the screen are analyzed and authenticated. According to Stanciu [4], this method is effective enough to protect the system from statistic attack. An improved version [5] of this method of authentication uses the combination of four aspects which are time, pressure, size and acceleration obtained from the sensor of the device when a user types in his password.

Besides password input, Cognitive authentication also includes drawing of patterns [6]. Recognition of shape drawing patterns [7] to authenticate a user is a strong and easy way to protect the user against password peeking attacks. Another kind of Cognitive authentication method [8] is through the user's pattern of walking. In this method, [9] users wear a movement tracker attached to their waist to track the user's continuous movement data. Besides that, a type of Cognitive biometrics authentication measures the usage pattern and geographical location of regular usage of a user with his smartphone. This method [10] measures the user-phone interaction activity such as the application usage,

location, communication and motion to detect anomaly intruder usage scenarios.

It is suitable for mobile devices to implement a Cognitive biometric authentication such as the graphical password authentication as there are external costs involved in purchasing devices with sensors. Graphical Password Authentication is an authentication method in the Cognitive Biometric Authentication category which is suitable for implementation in mobile devices compared to existing numerical passcodes.

Passwords in the form of graphics [11] are secure alternatives to numerical and text-based passwords, where the users are required to select pictures for authentication instead of keying in texts. Passwords in graphical format are much easier to remember compared to text-based passwords. Some studies of psychology [12] have identified that the human brain is way better in memorizing and recognizing visualized information such as pictures, compared to information in the form of text or speech. Pictures are increasingly used for the purpose of security compared to mere texts, as the range of texts and numbers is limited in comparison to pictures which are infinite.

B. Recognition-Based Techniques

One of the graphical password authentication technique is called the Recognition-Based Technique. For this technique, symbols, icons or images are selected by the users in a series as a password during registration, [13] where the users have to identify the same pictures they have selected during the authentication period. Based on Figure 1, Dhamija and Perrig [14], introduced a method of authentication using predefined images. Through this method, users are required to select their pre-selected pictures which they have defined during their registration from a set of random images to get authenticated by the system. However, this method is vulnerable to shoulder surfing attack.

Another example of recognition-based graphical authentication is called Passface™ as shown in Figure 2. This technique [15] will display nine faces on the screen and require the user to choose their pre-selected faces in four rounds, choosing one pre-selected face per round.

Fig. 1. Pre-Defined Image Selection.

Fig. 2. Passface Authentication Example.

In addressing the shoulder surfing issue with a graphical recognition authentication method, Haichang Gao, Xiyang Liu, and Ruyi Dai [16] introduced a shoulder surfing prevention method using invisible pattern drawing by swiping gestures to select a sequence of predefined images instead of tapping. An image chain in a story is used to remember the picture sequences to provide the user with the authentication. This method is less likely to be considered as it is vulnerable to shoulder surfing attacks as it is considerably easier to be identified compared to numbers.

C. Recall-Based Techniques

Another technique for Graphical Password Authentication is the Recall-Based Technique, which is based on pure recall and requires the users to recreate the graphics without any given tips or assisting reminders. However, users may find it hard to recall their password with this technique even though it is more secure than recognition-based technique. A technique called Syukri, by Ali Mohamed Eilejtlawi [17] requires the user to make a signature with a drawing with a stylus pen or mouse during registration, and authentication will be based on the same signature drawing.

A similar technique based on recall is enhanced with cues, where users are required to recreate a graphical password with the assistance of tips to enhance the accuracy of the password, where images will be provided to the users in which they must select specific points in the pictures in the right sequence. An example of this technique is a method introduced by S. Chiasson, P.C. van Oorschot, and R. Biddle [18], where the next picture on sequence is shown depending on the point of the previous click by the user. Every picture shown next to the previous picture based on a coordinate function of the point of click by the user of the current picture. A wrong selection of a point will cause the next picture to be shown wrongly, which prevents the attacker from guessing the password without knowing the right point for clicking. An example is shown in Figure 3.

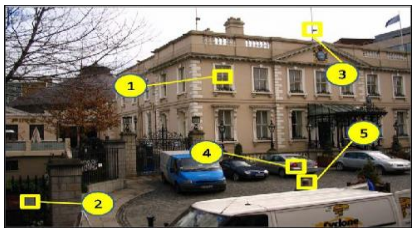

Fig. 3. Passpoint Example.

D. Hybrid Scheme

A combination of multiple graphical password authentication method forms a hybrid scheme. The hybrid scheme is proposed by researchers in addressing the issues with limitation in every graphical authentication technique like shoulder-surfing attacks, hotspot issues, and much more. H. Zhao and X. Li [19] introduced an example of a hybrid scheme, which is a text-in-graphic password authentication scheme - S3PAS in short, to counter shoulder-surfing attacks.

A combination of texts and graphics can resist shoulder surfing attacks, hidden cameras and spyware. The method of registration requires the user to choose "k", an original string text password. In the login authentication, the user has to look for the pre-defined password in the image, which will form an invisible triangle named the "passtriangle", and the user must then click in the region inside the invisible triangle to gain access as shown in Figure 4.

ChoCD is a hybrid graphical authentication system called ChoCD proposed by Radhi, R. A., Mohd, Z. J. [20]. ChoCD is a system which allows the user to sign in with a User ID and a graphical password as shown in Figure 5. The system is implementable in both desktop and smart phones. The system authenticates a user in three ways, from the first step based on choice selection to the second step based on clicks and thirdly based on drawings. The scheme only allows the authenticated user to be able to recognize the passwords through graphic, clicking positions and drawing patterns. Users should be able to remember the pattern when the images are shown.

Fig. 4. Passtriangle Scheme.

Fig. 5. ChoCD Hybrid Scheme Example.

III. The Coin Passcode Mobile Graphical Password Authentication Model

The Coin Passcode Graphical Password Authentication Model is a hybrid graphical password mobile authentication scheme. It is relatively swift to be inputted as a mobile device authentication mechanism compared to a four or six pins numerical passcode. The key feature of this model is its unique multi-elemental buttons which are resistance against shoulder surfing attacks and brute force attacks for mobile devices.

The identity verification of a smart device user will be done through the validation of a set of Coin Passcode Graphical Passwords Keypair Authentication process, where the user will initially register a set of Coin Passcode graphical password patterns to be remembered, and by inputting the correct sequence of coin passcode, patterned graphical passwords would authenticate the identity of the user based on their cognitive knowledge. This can prevent an unauthorized user from getting access to the mobile device from just spying.

A. The Coin Passcode Structure

The Coin Model Graphical Password Authentication uses the concept of multi-elements found in the structure of any currency coin. In coins from different countries, there is always a combination of different symbols, numerical values, and some wordings. As with the concept of coins, the Coin Model Graphical Password Authentication uses the element of colors, numerical values, and icons to form unique coin passcodes as shown in Figure 6. The colour codes are added in the Coin to assist color-blind users.

There are a total of 10 icons, ten numbers and ten colours used as the elements of the Coin Passcode. The list of the element items is illustrated in Figure 7. The icons are obtained from Google Material Icons for Android Development.

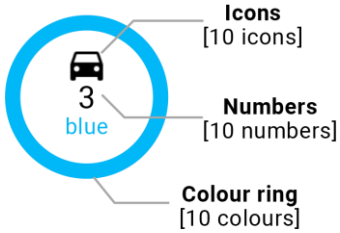

Fig. 6. The Coin Passcode Element Structure.

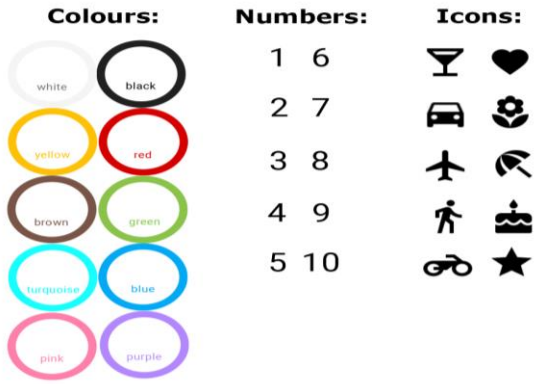

Fig. 7. The Coin Passcode Element List.

B. The Coin Passcode Keypad Randomization

The elements in the Coin Password are randomized each time, where every Coin Password will have a unique and different set of elements consisting of colors, numbers, and icons. There are a total of ten Coin Passwords in each different input attempt. With each Coin Password selected, a new layer will be formed, showing another randomized set of ten Coin Passwords, until the password authentication matches. An example of randomized Coin Passcode is shown in Figure 8, in which each attempt shows the number 3 with different colors and icon elements.

The randomization of the coin passcode sample is shown in Figure 9. The algorithm loops 6 times to randomize the keypad elements 6 times for all 6 inputs.

Fig. 8. Example of Coin Passcode Elements Randomization.

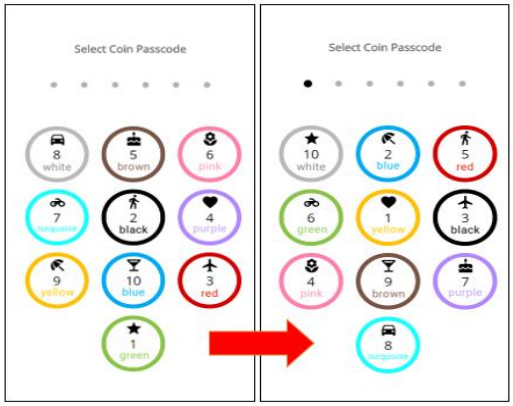

Fig. 9. Coin Passcode Shoulder-Surfing Proof Randomization Sample.

C. The Coin Passcode Registration

To strengthen the complexity of the Coin Password, a minimum password standard is set. Each of the three elements must be present in the Coin Password Combination at least twice, resulting in a combination of six coins in a passcode sequence with all three different hidden elements.

The Coin Passcode limits the user to place precisely six Coin Passcodes elements in the sequence during registration. The registering of the Coin Passcodes requires one secret hidden element item from each sequence to be initialized by the user during registration. For example, if the hidden element of the first Coin Password chosen is the color element 'Yellow', then the color 'Yellow' would be the key to the first Coin Password, ignoring the other two elements in the first Coin Password, which are the randomized numbers and icons as shown in Figure 10.

The registration algorithm limits the user to select all three different element items in the first three coin-passcodes element selection by removing an element to be selected after each selection. The algorithm then loops again for the last three coin-passcodes selections with the same limitation.

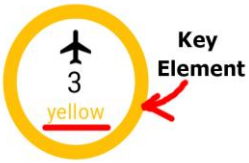

Fig. 10. The Key Element Example in Coin Passcode.

D. The Coin Passcode Authentication Algorithm

The Coin Graphical Password Authentication is designed in a way that only the authorized user knows the hidden element he or she registers out of the three elements in each coin, whether it's the color, number, or the icon.

An example of a Coin Passcode Registered Sequence combination is shown in Figure 11, with the first secret coin numerical element of "Three", a second coin with the secret color element "Yellow", and the third coin with the secret icon element "Car", continuing the rest of the three secret Coin Passcodes elements with the number "Five", the color "Blue", and finally the icon "Flower" respectively. The authentication system will then match the Coin Passcode inputs based on the registered Coin Passcode elements and sequence while ignoring the rest of the public elements in each of the six Coin Passcode inputs. Any other attempt by selecting coins without the elements in the right sequence will result in a failure in the identity authentication.

An object array is used to store the user's coin passcode login input to be matched with the registered coin passcode object array to check whether the login input object array contains the registered credentials in the right sequence for authentication.

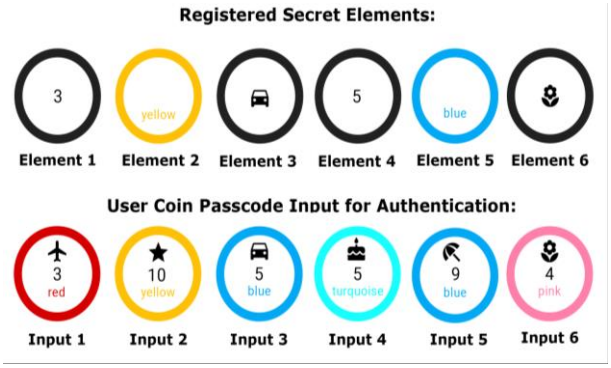

Fig. 11. Registered Secret Elements and Authentication Input Example.

IV. Security Analysis and Usability Metrics

A. Usability Metrics and Security Analysis

Several experiments are conducted with a group of 50 students to carry out the security analysis and usability metrics for the Coin Passcode against other similar mobile authentication models including the Numerical Passcode, Alphanumeric Passwords, and Passfaces™. The experiments conducted covers the usability metrics of login time and password memorability, and security analysis of shoulder surfing attack, password guessing attack and brute-force attack for each of the mentioned authentication models.

TABLE I. PASSWORD ATTACK COMPARISON TABLE

Name of Attacks	Password Schemes			
	Numerical Passcode	*Alphanumeri-cal Passcode*	*Passfaces™*	*Coin Passcode*
Shoulder-Surfing Attack	Y	Y	Y	N
Dictionary Attac	N		N	N
Password Guessing	Y	Y	Y	Y
Brute-force Attac	Y	Y	Y	N
Spyware Attack	Y	Y	Y	N

Table 1 summarizes the security of the different password schemes against several password attack methods. "Y" refers to Yes and it means that it is vulnerable to the forms of attack. While "N" refers to No and it means that the password scheme is secured against the attack type.

B. Password Complexity Comparison

The Coin Passcode Authentication Model which consists of three elements in each coin creates a cognitive authentication link between the user and the authentication system, where only the right user would know the secret element and sequence he or she sets, leaving the rest of the people confused about the password.

Based on the calculations below, the complexity of the Coin Passcode Model is much more resistant to brute force attacks compared to Numerical Passcodes and Passfaces, but weaker compared to Alphanumerical Password due to the differences in the number of elements. The complexity comparison chart of Coin Passcode and Numerical Passcode can be seen in Figure 12.

It takes 729 million attempts to brute force a triple elemental Coin Passcode in the right sequence to find out the right combination of the Coin Passcode secret element values. This makes guessing the password way more difficult compared the huge difference in passcode combination possibilities.

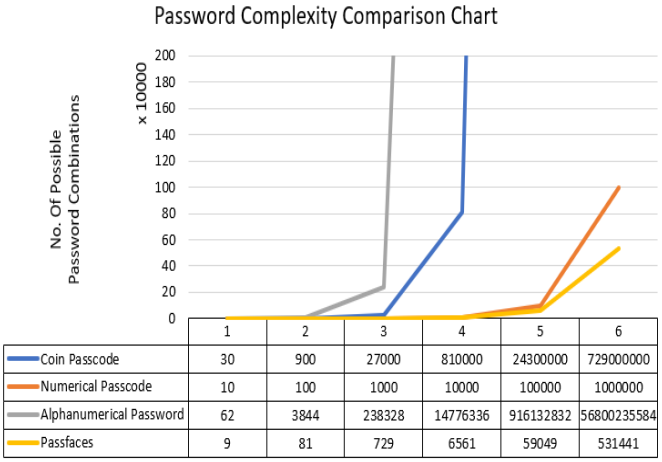

Fig. 12. Password Complexity Comparison Chart.

(N x E) ^{L} ***= No. of Possible Passcode Combinations,***
N = No. of Input Buttons, E = No. of Elements,
L = Length of Passcode

$(10 \times 3)^{6} = 729{,}000{,}000$ Coin Passcode Combinations (1)
$(10 \times 1)^{6} = 1{,}000{,}000$ Numerical Passcode Combinations (2)
$(62 \times 1)^{6} = 56{,}800{,}235{,}584$ Alphanumerical Combinations (3)
$(9 \times 1)^{6} = 531{,}441$ Passfaces™ Password Combinations (4)

C. Shoulder Surfing Attack and Spyware Attack

Shoulder Surfing attack uses the technique of direct observation or through recording using video cameras such as high-resolution surveillance equipment or hidden cameras to obtain a user's credentials. A spyware attack is when malwares are installed in a user's device to record the user's credentials input, while the information is sent back to the attacker for exploitation. Both of these attacks can easily obtain and exploit a user's numerical and alphanumerical password, or Passfaces™ credentials by directly observing the password input pressed by the user. However, the Coin Passcode is resistant to this type of attack.

An experiment is conducted with a group of 50 students, where a set of passwords for different authentication models, each with an equal password length of six items is pressed in front of the students through a big screen, with each button pressed at five-second intervals. The students are then asked to retype or reselect the shoulder surfed passwords. The result of the shoulder surfing attack experiment is shown in Figure 13. The numerical passcode and alphanumerical password are seen to have a high rate of shoulder surfing success due to their vulnerability to this attack method. The Passfaces™, however has a lower success rate as it requires a certain recognition and memorability of the level of the faces used to reselect the right one.

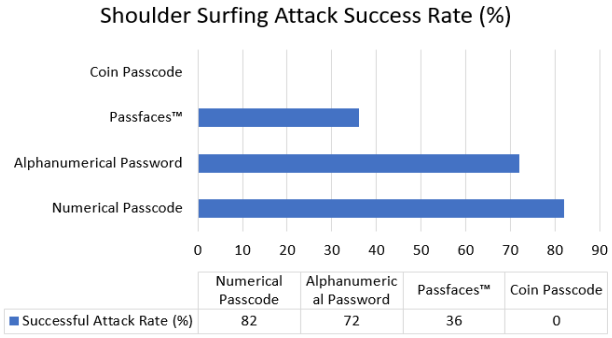

Fig. 13. Shoulder Surfing Attack Success Rate Chart.

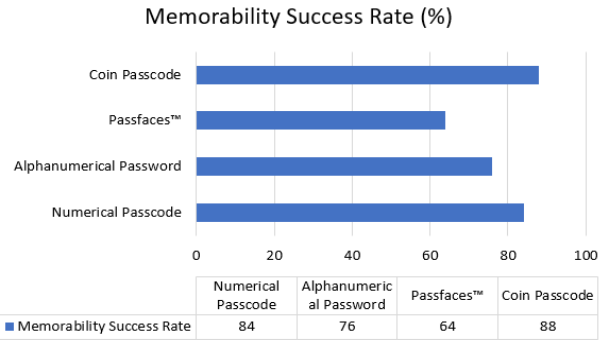

Fig. 14. Password Memorability Success Rate Chart.

The Coin Passcode can be observed to have zero success rate of shoulder surfing attack. This is because having multiple graphical elements in each input of the Coin Passcode would make shoulder surfing attack and spyware attack meaningless, as students do not get any direct password information from just observing the Coin Passcode combination inserted by the user. It is designed so that it is impossible for a shoulder surfer to know which secret element out of the three was the one being chosen by the user in a single input button.

Memorability is the measurement of the extent to which the users can remember the password after a period. A password memorability experiment is conducted for each of the four password authentication models. The test is conducted with a group of 50 students, where each student is given a similar set of passwords of the same password length of six for each password model. The students were given five minutes to memorize each password and were then shown a 3 minutes video to simulate an extended period of idle time. After the video ended, the students were asked to produce the same password in one-minute. The result of the experiment is shown in Figure 14.

The experiment result shows that the Coin Passcode has the highest memorability success rate followed by the numerical passcode, the alphanumerical password and lastly, the Passfaces™.

Based on the experiment, it was much easier to remember the Coin Passcode because the secret elements used are straightforward elements like colours, numbers, and icons, which can form a story-like chain of keywords such as "3 blue cars, 5 red bikes", as compared to remembering numbers, words or faces which have no direct meaning or connection to the tester. The experiment found that unfamiliar faces are hard to remember after a period of idle time, even though it is also a form of graphical password.

D. Login Time

Login Time refers to the time taken for users to log into the authentication system using their credentials. An experiment is conducted to analyze the login time for the four authentication models. The test is conducted with a group of 50 students, where each student is given a set of similar passwords of the same length of six for each password model. The students are then asked to reproduce the same passwords five times, and each login attempt time was recorded. The result of the experiment is shown in Figure 15.

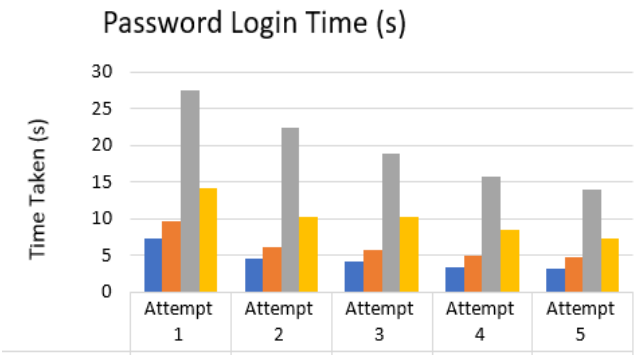

Fig. 15. Password Login Time Chart.

The Coin Passcode has slightly longer login time compared to Numerical Passcode and Alphanumerical Password of the same length even after five attempts. This is because the positioning of the numerical passcode and alphanumerical password are fixed, which the test user can simply memorize and get used to from each increased attempt. However, the positioning of the Coin Passcode elements is randomized and shuffled in each attempt, which is designed to confuse the shoulder surfing attacker, causing a longer login time for the test users. The Passfaces™ takes a much longer login time compared to the other password models due to the low memorability of the unfamiliar faces which requires the test user to take time to confirm the faces.

E. Password Guessing and Dictionary Attack

Password Guessing is a kind of brute force attack which uses knowledges or hints gained from the password owner. Each of the password models mentioned in the analysis are vulnerable to this attack when the user leaves certain hints or information about their password exposed to the attacker. This attack cannot be avoided and can only be prevented through security awareness and training.

A dictionary attack is conducted using a list of frequently used words or number patterns to crack the password efficiently. However, this only applies to the existing Numerical Passcodes and Alphanumerical Passwords due to the reason that these passwords often contain phrases that are predictable and highly used statistically. The Coin Passcode Authentication Model and the Passfaces™ is not applicable for dictionary attack, because these two authentication models does not contains text or words that can be prepared in dictionary attack.

V. Discussions

Most graphical passwords currently available are mostly proven to be more secure and resistant to several cybersecurity attacks compared to existing numerical and alphanumerical passwords. However, these graphical passwords are mostly available only in the field of research, education and theoretical discussion, and are rarely implemented practically. It may be due to several poor usability factors such as low memorability, high login time, and non-user friendly or non-mobile friendly interfaces, compared to the existing numerical and alphabetical password authentication methods.

The proposed Coin Passcode is shown to have higher password complexity when compared to its closest identical numerical passcode model. Even though the alphanumeric password model has a higher password complexity, it is still not a completely secure password mechanism due to its vulnerability towards shoulder surfing attacks. The Coin Passcode is designed to overcome the shoulder surfing attack vulnerability and is currently designed specifically for a swift mobile authentication which greatly enhances the password complexity compared to its nearest comparison. A higher password complexity can be achieved when the coin passcode's multi-elemental concept is implemented to a similar input of alphanumerical passwords.

The memorability of the Coin Passcode is also a beneficial key feature due to its straightforward elemental attributes

which can be formed into a chain of story-like keywords that other existing password models are missing. It is more likely for people to remember a story formed by visuals rather than numbers or alphabets. The login time for the Coin Passcode is not as fast as the existing password models due to the randomization and element shuffling nature of the Coin Passcode model. However, this can be considered a security over performance prioritization measure.

VI. Conclusion

In conclusion, the Coin Passcode is able to overcome the current shoulder-surfing and spyware attack vulnerability that existing mobile application numerical passcode authentication layers suffer from. It is shown that having a Multi-elemental passcode for a mobile login interface can prevent direct observation password attacks, and at the same time provide a higher password complexity against brute-force and password guessing attacks. It is a combination of the behavioral context uniqueness of each person that makes this multi-elemental passcode a stronger mobile password interface.

The authors believe in the real potential of graphical password in benefiting the current mobile smart devices swift authentication mechanism, in terms of usability and security aspects. This brings the purpose for us to propose the Coin Passcode Graphical Password Mobile Authentication Model in hoping to overcome the challenges by bringing a simplicity in usage plus complexity in security for the mobile developers as well as the mobile users. However, there are still limitations in the current proposed design of the Coin Passcode which can be further enhanced in the future for the betterment of mobile security. One of it is the lack of encryption for the coin passcodes input and stored passcodes, as the elements are currently stored purely in plaintext and can be easily modified via code injection attack. The Multi-elemental input concept should also be further explored in password model fields other than mobile security layers, such as the network security and banking security.

Future work

The authors believe that the graphical password implementation has a great potential for different applications besides of mobile devices due to its feautes such as secure, and ease of use. Authors will extend this model of other application areas in future.

References

[1] Spolaor, R., Li, Q. Q., Monaro, M., Conti, M., Gamberini, L., Sartori, G. Biometrics Authentication Methods on Smartphones: A Survey. PsychNology Journal, Nov. 2016, Volume 14, Number 2-3, 87-98.

[2] Clarke, N. L., and Furnell, S. M. Authenticating mobile phone users using keystroke analysis. International Journal of Information Security, 6(1), 1-14. New York: Springer International Publishing. 2007.

[3] Giuffrida, C., Majdanik, K., Conti, M., and Bos, H. I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics. In L. Cavallaro (Eds.) International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 92-111). New York: Springer International Publishing. Jul. 2014.

[4] Stanciu, V. D., Spolaor, R., Conti, M., and Giuffrida, C. On the effectiveness of sensor-enhanced keystroke dynamics against statistical attacks. In C. Busch and A. Brömme (Eds.) Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy (pp. 105-112). New York: ACM. Mar. 2016.

[5] Zheng, N., Bai, K., Huang, H., and Wang, H. You are how you touch: User verification on smartphones via tapping behaviors. In J. Kaur and G. Rouskas (Eds.) 2014 IEEE 22nd International Conference on Network Protocols (pp. 221-232). New York: IEEE. Oct. 2014.

[6] De Luca, A., Hang, A., Brudy, F., Lindner, C., and Hussmann, H. Touch me once and I know it's you: implicit authentication based on touch screen patterns. In J. A. Konstan, E. H. Chi and Kristina Höök (Eds.) Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 987-996). New York: ACM. May 2012.

[7] De Luca, A., Harbach, M., von Zezschwitz, E., Maurer, M. E., Slawik, B. E., Hussmann, H., and Smith, M. Now you see me, now you don't: protecting smartphone authentication from shoulder surfers. In M. Jones and P. Palanque (Eds.) Proceedings of the 32nd annual ACM conference on Human factors in computing systems (pp. 2937-2946). New York: ACM. Apr. 2014.

[8] Mantyjarvi, J., Lindholm, M., Vildjiounaite, E., Makela, S. M., and Ailisto, H. A. Identifying users of portable devices from gait pattern with accelerometers. In Petropulu (Eds.) Proceedings (ICASSP'05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005. (Vol. 2, pp. ii-973). New York: IEEE. Mar. 2005.

[9] Derawi, M. O., Nickel, C., Bours, P., and Busch, C. Unobtrusive user authentication on mobile phones using biometric gait recognition. In D. W. Fellner, X. Niu (Eds.) Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP) (pp. 306-311). New York: IEEE. Oct. 2010.

[10] Shi, E., Niu, Y., Jakobsson, M., and Chow, R. Implicit authentication through learning user behavior. In S. K. Bandyopadhyay and W.Adi (Eds.) International Conference on Information Security (pp. 99-113). Berlin: Springer Berlin Heidelberg. Oct. 2010.

[11] De Angeli, L. Coventry, G. Johnson, and K. Renaud. Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. 2005. International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 128–152.

[12] Kirkpatrick. “An experimental study of memory,” 1894. Psychological Review, vol. 1, pp. 602–609.

[13] K. Renaud and E. Smith. Jiminy. “Helping user to remember their passwords”. Technical report, School of Computing, Univ. of South Africa. 2001.

[14] R. Dhamija, and A. Perrig. “Déjà Vu: A User Study Using Images for Authentication”. In 9th USENIX Security Symposium. 2000.

[15] Grinal, T., Aakriti, T., Akshata, S., Malvina, R., Aishwarya, S. Graphical password authentication using Pass faces. Mar. 2015. Int. Journal of Engineering Research and Applications, Vol. 5, Issue 3, Part 5, pp.60-64.

[16] Haichang Gao, Xiyang Liu, Ruyi Dai. “Design and Analysis of a Graphical Password Scheme”, International Conference on Innovative Computing, Information and Control (ICICIC), pp. 675 – 678. 2009.

[17] Ali Mohamed Eilejtlawi. “Study and development of a new graphical password system”. May 2008.

[18] S. Chiasson, P.C. van Oorschot, and R. Biddle. “Graphical password authentication using Cued Click Points”. In European Symposium On Research In Computer Security (ESORICS), LNCS 4734, pp. 359-374. Sep. 2007.

[19] H. Zhao and X. Li. “S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme”, in 21st International Conference on Advanced Information Networking and Applications Workshops, vol.2. Canada, pp. 467-472. 2007.

[20] Radhi, R. A., Mohd, Z. J. ChoCD: Usable and Secure Graphical Password Authentication Scheme. Indian Journal of Science and Technology, Vol 10(4), DOI:10.17485. Jan. 2017.