International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

MULTI-FACTOR AUTHENTICATION BASED ON GAME MODE FOR ANDROID APPLICATION

Isswarya Murugan[1], Manimekalai. S[2], Mounika. G[3], Anand. C[4]

[1,2,3]Students, Department of Information Technology, Jeppiaar SRR Engineering College, Chennai, Tamil Nadu, India.
[4]Assistant Professor, Dept. of Information Technology, Jeppiaar SRR Engineering College, Chennai, Tamil Nadu, India

---

Abstract - *There are no simple solution for authentication exists to achieve security and memorability. In order to occur these goals, we propose a Multi-fAcet Password Scheme (MAPS) for mobile authentication. This MAPS combines the information from multiple facets to form a password, which allows MAPS to enlarge the password space and improve memorability by reducing memory interference. Based on this, we implement a Chess-based MAPS (CMAPS) for Android systems. Only two and six gestures are required for CMAPS to generate passwords with better security strength than 4-digit PINs and 8-character alphanumeric passwords, respectively. Our user studies show that CMAPS can achieve high recall rates while exceeding the security strength of standard 8-character alphanumeric passwords used for secure applications.*

Key Words: *Authentication, human computer interaction, graphical user interfaces.*

1. INTRODUCTION

The popularity of mobile devices is due to ubiquitous Internet access through communication technologies such as WiFi and 4G/LTE, easy to use numerous applications and games. In meantime, the security of mobile devices is becoming a major concern as device users are storing sensitive data such as personal contacts and utilizing sensitive information. Authentication, the first defense mechanism preventing unauthorized access to a mobile device, allows owners of mobile devices to unlock and use their devices. Designing an authentication for mobile devices is a challenging task because the scheme should be secure, capable of generating human-memorable passwords, and usable.

A secure authentication scheme should have a large password space, i.e., a large number of possible passwords. In this paper, we separate memorability from usability to give importance for memorability. It has been recognized that no silver bullet exists to achieve both security and memorability. Obviously with the addition of a usability requirement, the task becomes even more challenging. The alphanumeric password scheme, which has been used for decades for various computer systems, is not suitable for mobile authentication. Most mobile devices support the touch based soft keyboard, which replaces the hardware keyboard. Due to the limited size of the soft keyboard, text input is relatively slow and typo-prone, leading to frustrating usability issues. Poor usability, can lead to users choosing short or easy to type passwords as a workaround.

We are proposing the concept of Multi-fAcet Password Scheme (MAPS) for mobile authentication. Instead of repeating the same type of information, such as characters in alphanumeric passwords and dot connections in Google's pattern unlock, MAPS combines information from multiple facets, i.e., multiple types of information, to generate passwords. Because of combining information from multiple facets, MAPS can generate a huge number of passwords

Based on the idea of MAPS, we design and implement a Chess-based MAPS (CMAPS) as an example of MAPS. We formally analyze the security strength of CMAPS and prove that CMAPS is more secure than existing mobile authentication schemes. Only two and six gestures are required for CMAPS to get passwords with higher security strength than 4-digit PINs and 8-character alphanumerical passwords severely. The advantage is because CMAPS can fuse information from multiple facets through a single gesture and using multiple facets can significantly enlarge the password space.

2. RELATED WORK

In this section, we review related work on graphical passwords, mobile authentication, and gamification.

2.1 Graphical password

The original proposal for the graphical password is the US patent filed by Blonder [5] in 1996. Blonder's implementation shows users a number of ''tap regions'' in a predetermined image, and requires users to set a password by arranging these regions by location and sequence. It was inferred that a graphical approach provides better memorability than traditional passwords because the human brain is relatively weak at remembering sequences of numbers or letters, but good at processing visual data [5], [6]. As graphical authentication schemes gained popularity, they were grouped into three categories: recognition-based schemes, recall-based schemes, or cued-recall schemes [9]. The classification is based on memory tasks as outlined in

[10]. These three memory operations are handled in different ways.

Recall-based schemes: Draw-A-Secret [6], ask users to reproduce a secret drawing or gesture, typically with a touch screen or pointing device. Users create a Draw-A-Secret password by drawing a gesture on their touch screen PDA, and authenticate themselves by reproducing it. A gesture is considered a line drawn along the screen.

Cued-recall schemes: It require users to perform actions on specific locations of an image or screen. Users of Passpoints are asked to specify ''click-points,'' areas that need to be touched, in a pre-defined image. Authentication is achieved by touching all of the click points in the image. The idea is that a user can chose a personal image, for example a picture of a star, and chose click points that are memorable or meaningful to the user, for example the points of the star.

PicassoPass is another cued-recall scheme, asks users to recall one piece of visual information from up to five different layers (color, image, letter, location, and shape). For example, a word could encompass the choices: red, top left corner, circle. Layers are superimposed over each other during authentication. The user effectively picks one value from one dimension (layer) at a time to authenticate, while other dimensions are used as distractions for potential observers.

2.2 Mobile Authentication

Various authentication schemes have been implemented in mainstream smartphone operating systems. The existing authentication schemes trade security for memorability and usability.

Four-digit PIN is entered on a classic PIN pad displaying the digits 0-9. Thus only 10,000 passwords are possible. This scheme is clearly intended only to discourage unauthorized use by adversaries who lack time or dedication. Zezshwitz et al. developed SwiPin [18], a scheme based on PINs which takes advantage of gesture recognition capabilities on mobile devices for input rather than classic button pressing.

Pattern unlock scheme presents a user with a 3 × 3 grid of dots.1 Similar to Draw-A-Secret, a user creates 1A larger gird is possible in recent versions of the Android operating system. We specialize on the default size of the grid during this paper. Our analysis and conclusion discussed below still holds for larger grids. a watchword by drawing lines connecting the dots in a certain way. A valid pattern must consist of at least 4 dots, connected only by. But the total number of possible patterns in a 3 × 3 grid is only 389,112.

The picture authentication scheme developed for users to upload an image and create a password by drawing a series of three gestures on the image. For example, the password could consist of drawing a circle in the center of the screen, then a diagonal line connecting two corners, then a tap in the center of the screen. The direction of the circle (e.g. clockwise vs counterclockwise) is significant, as well as the direction the lines are drawn. Naturally, a certain amount of inaccuracy is permitted when drawing the gestures. There are roughly 109 picture passwords using 3 gestures or less and 6∗1011 picture passwords using 4 gestures or less.

2.3 Gamification

Gamifying security is an idea that seeks to tie security mechanisms to games in order to improve security, memorability, and usability. For example, the Pass-Go graphical system is based on the board game GO [7]. Hamari et al. [8] propose that gamifying an experience can produce positive effects in learning and user experience. Kroeze and Olivier [9] proposes that gamifying authentication can enhance security via improved user behavior. In this paper, we propose CMAPS, an implementation of MAPS based on the chess game. Using CMAPS does not require any knowledge of chess. In other words, anyone without any knowledge of chess can use CMAPS easily, but players of chess may experience the benefits of gamification.

3. THREAT MODEL

We assume the attacker are interested in accessing a mobile device for sensitive data or sensitive applications installed on the mobile device. We also make the following assumptions on the attacker's capability:

1) We assume the attacker has physical access to the mobile device because (a) the mobile device is stolen, (b) the mobile device is decommissioned, or (c) simply the owner is away from the mobile device.

2) We assume that the attacker cannot simply disassemble the mobile device and obtain the sensitive data or sensitive applications from the storage taken out of the device for various reasons such as device encryption.

3) We assume that the attacker cannot obtain the sensitive data through network connections over Wifi or 3G/4G communications.

4) We assume that the device owner cannot or has not yet wiped the device remotely through device protection features such as the remote erase feature supported by Apple's Find My iPhone/iPad service.

4. PROPOSED SYSTEM

We propose a Multi-facet Password Scheme (MAPS) for mobile authentication. MAPS fuses information from multiple facets to form a password, allowing MAPS to enlarge the password space and improve memo ability by reducing memory interference, which impairs memory performance according to psychology interference theory. The information fusion in MAPS will increase usability, as fewer input gestures are required for passwords of the same

security strength. Based on the idea of MAPS, we implement a Chess-based MAPS (CMAPS) for Android systems. Only two and six gestures are required for CMAPS to generate passwords with better security strength than 4-digit PINs and 8-character alphanumeric passwords, respectively. Our user studies show that CMAPS are able to do high recall rates while exceeding the security strength of standard 8-character alphanumeric passwords used for secure applications.

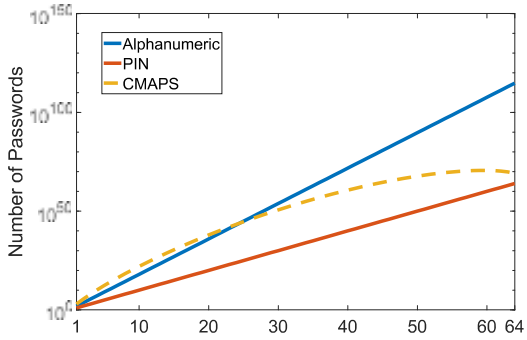

Figure 1: Number of passwords supported by different number of gestures

A CMAPS user sets a password by placing chess game pieces onto a classical chess game board with 8 8 tiles. The resulting chess formation is a CMAPS password. When the user wants to unlock the mobile device later, CMAPS will display a blank chess board and the chess game pieces. The user can try to unlock the system by placing the game pieces back onto the game board. If the chess formation input by the user is exactly the same as the formation set in the password setting phase, the mobile device will be unlocked. A user can put a game piece onto the chess board with one gesture connecting a selected game piece to a desired tile in the board. No knowledge of chess is required to use CMAPS as (1) CMAPS allows any game piece to be placed on any tile in the chess board and (2) CMAPS allows any possible chess formation including those illegal in a chess game such as a formation with more than two kings. The design is to allow a user without any chess knowledge to use CMAPS. We also hypothesize that chess skills may help to memorize passwords because a user may use a favorite chess formation or a formation with some game pieces related by attacking or defending for better memorability.

As an example of MAPS, CMAPS fuses information from multiple facets. The facets used in CMAPS, as shown in Table 1, include the color of the game piece (black or white), the type of the game piece (king, queen, rook, bishop, knight, or pawn), and the location of the game piece (the row of the desired tile and the column of the desired tile). CMAPS fuses the information from these facets with one gesture on a touch screen that simply puts a game piece onto a chess board.

We analyze the usability of CMAPS and compare CMAPS with other password schemes in terms of usability. CMAPS satisfies the same set of usability requirements as existing graphical password schemes on mobile devices such as the pattern unlock scheme and the picture password scheme.

Table -1: Number of Gestures Required for Different Password Strength. (For fair comparison, we remove the limit on the number of digits in a PIN and the number of dots in the pattern unlock scheme. The numbers for the pattern unlock are the lower bounds of segments between successive dots required to achieve different password strength as we assume it is possible to connect one dot with any other dot in a grid for simplification. The numbers for alphanumeric passwords are also the lower bounds as we assume that an alphanumeric password of l characters can be completed in l gestures. In reality a user will need to use an extra gesture to press the shift key or switch from the letter keyboard to the symbolic keyboard.)

Number of Passwords	10^{10}	10^{20}	10^{30}	10^{40}	10^{50}
PIN	10	20	30	40	50
Alphanumeric	6	12	17	23	28
Pattern Unlock	12	23	34	45	56
CMAPS	4	9	15	22	30

4.1 User Registration and Login

The user who is going to use the authentication scheme has to do registration. Whenever new registration is initiated the user has to enter their basic details . Once when the user enters into the system with the registered credentials the system allows the user to Gesture registering Module.

Figure 2: Screenshot of User registration and Login page

4.2 Single-Hand Gesture

When the user has to register with the gesture , they has to move finger over the touchscreen without taking away the finger. The OTP verification will be done where, OTP will be received to user's registered mobile number. Once when the gesture function get over the session get completed and the new single hand gesture password will be stored in the database as encrypted.

4.3 Multi-Hand Gesture

When the user has to register with the gesture , they has to move finger over the touch screen step by step taking away the finger multiple times. Once when the gesture function get over the session get completed and the new multi hand gesture password will be stored in the Database encrypted.

Figure 3: Screenshot of Single and Multi Hand Features

4.4 Forget Password Gesture

When the user does not able to recognize the registered password they can opt for forget password. Once again the OTP will be received to the registered user's mobile. When the user is authenticated the CMAPS system will allow for new password registration.

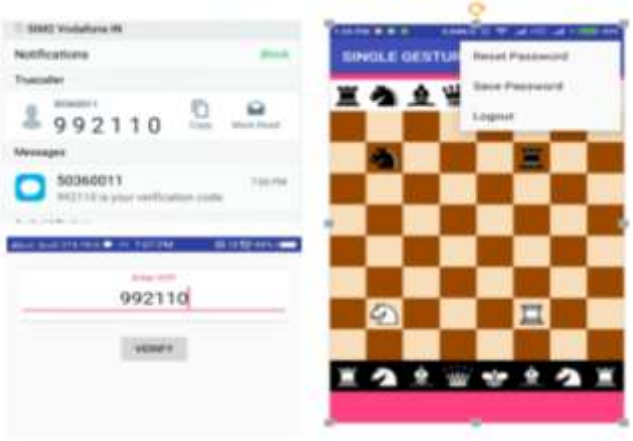

Figure 4: Screenshot of User opting for password with help of OTP

5. ADVANTAGE

MAPS can reduce memory interference greatly so, MAPS's using information from multiple facets leads to both better security strength and less memory interference. MAPS can generate huge amount of possible passwords. When we formally analyze the security strength of CMAPS and prove that CMAPS is more secure than existing mobile authentication schemes.

The advantage is because CMAPS can fuse information from multiple facets through a single gesture and using multiple facets can significantly enlarge the password space.

6. CONCLUSION

In this paper, we propose MAPS for mobile authentication. MAPS can improve security, memorability, and usability jointly. MAPS fuses information from multiple facets to form a password. Using information from multiple facets can improve security strength by enlarging the password space and improve memorability by reducing memory interference. The graphical hints can help users to memorize passwords. Based on the idea of MAPS, we implemented CMAPS for Android devices and conducted a user study on CMAPS with the implementation. The user study shows that CMAPS, with security strength exceeding the strength current mobile authentication schemes and exceeding the requirements of banking, can achieve high recall rates. CMAPS enhances usability by requiring significantly fewer touch gestures than other schemes to achieve an equivalent password space.

REFERENCES

[1] This work was supported in part by the Faculty Development Award from Cleveland State University and in part by the U.S. National Science Foundation under Grant CNS-1338105, Grant CNS-1343141, Grant CNS-1460897, Grant DGE-1623713, and Grant DGE-1821775.

[2] F. Alt, S. Schneegass, A. S. Shirazi, M. Hassib, and A. Bulling, ''Graphical passwords in the wild: Understanding how users choose pic- tures and passwords in image-based authentication schemes,'' in Proc. 17th Int. Conf. Hum.-Comput. Interact. Mobile Devices Services, 2015, pp. 316–322.

[3] P. Manning, C. T. McLennan, and Y. Zhu, ''Authentication method for a computing device using interactive game board and game piece images,'' U.S. Patent 61 782 062, 2013.

[4] H. Gao, Z. Ren, X. Chang, X. Liu, and U. Aickelin, ''A new graphical password scheme immune to shoulder-surfing,'' in Proc. Int. Conf. Cyberworlds, Oct. 2010, pp. 194–199.

[5] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, ''The design and analysis of graphical passwords,'' in Proc. 8th Conf. USENIX Secur. Symp., 1999, pp. 1–15.

[6] M. A. Defeyter, R. Russo, and P. L. McPartlin, ''The picturesuperiority effect in recognition memory: A developmental study using the response signal procedure,'' Cogn. Develop., vol. 24, no. 1, pp. 265–273, 2009.

[7] T. S. Tullis, D. P. Tedesco, and K. E. McCaffrey, ''Can users remember their pictorial passwords six years later,'' in Proc. Extended Abstr. Hum. Fact. Comp. Syst., 2011, pp. 1789–17

[8] G. E. Blonder, ''Graphical password,'' U.S. Patent 5 559961 A, Sep. 24, 1999.

[9] J. Hamari, J. Koivisto, and H. Sarsa, ''Does gamification work?—A lit- erature review of empirical studies on gamification,'' in Proc. IEEE 47th Hawaii Int. Conf. Syst. Sci. (HICSS), Jan. 2014, pp. 3025–3034. C. Kroeze and M. S. Olivier, ''Gamifying authentication,'' in Proc. IEEE Inf. Secur. South Africa (ISSA), Aug. 2012, pp. 1–8.

BIOGRAPHIES

Isswarya Murugan

Pursuing B.Tech degree in Information Technology from Jeppiaar SRR Engineering College, Chennai,Tamil Nadu.

Manimekalai. S

Pursuing B.Tech degree in Information Technology from Jeppiaar SRR Engineering College, Chennai,Tamil Nadu.

Mounika.G

Pursuing B.Tech degree in Information Technology from Jeppiaar SRR Engineering College, Chennai,Tamil Nadu.

Anand.C

Working as Asst.Professor in Jeppiaar SRR Engineering College, Chennai, TamilNadu.