9-28-2018

CMAPS: A Chess-Based Multi-Facet Password Scheme for Mobile Devices

Ye Zhu
Cleveland State University, y.zhu61@csuohio.edu

Jonathan Gurary
John Carroll University

George Corser
Saginaw Valley State University

Jared Oluoch
University of Toledo

Nahed Alnahash
Oakland University

See next page for additional authors

Received July 1, 2018, accepted September 16, 2018, date of publication September 28, 2018, date of current version October 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2872772

CMAPS: A Chess-Based Multi-Facet Password Scheme for Mobile Devices

YE ZHU[1], (Member, IEEE), JONATHAN GURARY[2], GEORGE CORSER[3], (Member, IEEE), JARED OLUOCH[4], NAHED ALNAHASH[5], HUIRONG FU[5], (Member, IEEE), AND JUNHUA TANG[6]

[1]Department of Electrical Engineering and Computer Science, Cleveland State University, Cleveland, OH 44115, USA
[2]John Carroll University, University Heights, OH 44118, USA
[3]Department of Computer Science and Information Systems, Saginaw Valley State University, Saginaw, MI 48603, USA
[4]Department of Engineering Technology, University of Toledo, Toledo, OH 43606, USA
[5]Department of Computer Science and Engineering, Oakland University, Rochester, MI 48309, USA
[6]School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

Corresponding author: Ye Zhu (y.zhu61@csuohio.edu)

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.

ABSTRACT It has long been recognized, by both security researchers and human–computer interaction researchers, that no silver bullet for authentication exists to achieve *security*, *usability*, and *memorability*. Aiming to achieve the goals, 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 memorability by reducing memory interference, which impairs memory performance according to psychology interference theory. The information fusion in MAPS can 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 can achieve high recall rates while exceeding the security strength of standard 8-character alphanumeric passwords used for secure applications.

INDEX TERMS Authentication, human computer interaction, graphical user interfaces.

I. INTRODUCTION

This paper studies authentication on mobile devices with touch screens. As mobile devices such as smartphones become increasingly popular, so does the realization that security is an important requirement for the use of mobile devices in our daily life. In 2013, annual worldwide smartphone shipments topped 1 billion for the first time [1]. The popularity of these mobile devices is due to a unique set of features including ubiquitous Internet access through communication technologies such as Wifi and 4G/LTE, easy to use touch-based inputs, and numerous applications and games. In the 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 applications like banking and stock trading.

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 scheme 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. Obviously the passwords generated by the scheme should also be easy to remember. In this paper, we separate memorability from usability to emphasize the importance of memorability. It has long been recognized that no silver bullet exists to achieve both security and memorability [2]. 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. The scheme generally requires a keyboard for quick input of alphanumeric passwords. However, most current mobile devices are not equipped with a hardware keyboard. Instead, most mobile devices support the touch

based soft keyboard, which replaces the hardware keyboard with an on-screen image map of keys. Due to the limited size of the soft keyboard, text input is relatively slow [3] and typo-prone, leading to frustrating usability issues. Poor usability, in turn, can lead to users choosing short or easy to type passwords as a workaround.

In this paper, we propose the 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. Passwords generated by MAPS are easy to remember because (1) MAPS is an authentication scheme based on graphical passwords, which have been proven easier to remember than alphanumeric passwords [4], (2) MAPS can fuse information from multiple facets through a single gesture on the touch screen, (3) MAPS can greatly reduce memory interference, a psychology effect leading to forgetting, and (4) graphical hints designed for MAPS can further increase the memorability of passwords. MAPS is also easy to use on mobile devices since passwords generated by MAPS can be input on touch screens with just a small number of gestures.

The contributions made in this paper are summarized as follows:

- We propose a Multi-fAcet Password Scheme (MAPS) for mobile authentication. MAPS can generate a huge amount of possible passwords. MAPS is also easy to remember and easy to use on mobile devices. 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 2 and 6 gestures are required for CMAPS to generate passwords with better security strength than 4-digit PINs and 8-character alphanumeric passwords respectively. 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.
- We formally analyze the usability of CMAPS and show that CMAPS has better usability, since one gesture in CMAPS brings a larger amount of information than other schemes.
- Our user studies show that CMAPS, with security strength exceeding the strength of current mobile authentication schemes and exceeding the requirements of banking, can achieve high recall rates after one week.

The rest of the paper is organized as follows: Section II reviews related work on graphical passwords, mobile authentication, and memory interference. In Section III, we outline the threat model considered in this paper. In Section IV, we formally define the key criteria for mobile authentication methods. In Section V, we first present the design of MAPS and then use CMAPS as an example to explain the rationales behind the design. In Section 6, we theoretically analyze the security strength and usability of CMAPS. Section VII presents our user studies on the memorability and usability of CMAPS. In Section VIII, we discuss the user studies and possible extensions of MAPS. We conclude the paper in Section IX.

II. RELATED WORK

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

A. GRAPHICAL PASSWORDS

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. These regions are then hidden from view, leaving only the original reference image. To re-authenticate, the user must select the "tap regions" in the same 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]. That assumption was based on the *picture superiority effect*, the notion that humans have a much greater capacity for processing and remembering visual data than numbers and letters [7]. This hypothesis was eventually supported by further research [4]. Tullis *et al.* [8] shows that graphical passwords can remain memorable even years after they are no longer in use. CMAPS is also one type of graphical password schemes. In addition CMAPS further enhance memorability by reducing memory interference through combining multiple facet information.

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. In recognition, the subject is tasked with merely identifying if something is familiar, for example asking a person if they have seen a certain picture before. Recall requires accessing something directly from memory, a more challenging task, for example asking a person to reproduce a drawing they once made. Cued-recall provides a hint, such as the background of the drawing, but again requires the subject to draw up something from memory.

In recognition-based schemes, such as Deja Vu [11], the user is prompted to identify previously selected images. Users initially create a portfolio of images, taken from a large set of abstract images consisting of basic fractal and color patterns. To authenticate themselves, users must pick images from their portfolio out from a number of decoy images. Passface [12] is a commercial example of recognition-based authentication built for the open market. This software works

largely in the same way as Deja Vu, except that pictures of human faces are used in place of abstract images. Some research has suggested that using familiar imagery such as human faces weakens graphical schemes, as it opens them up to various selection biases [13]. Other research has found that people prefer faces from certain groups, for example elderly people remember PassFaces passwords better when faces of older people are used [14]. Our scheme uses common imagery that should not have any age, gender, or cultural biases.

Recall-based schemes, such as 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. Xside [15] is a more recent drawing-based scheme designed for touchscreen devices.

Cued-recall schemes, such as Passpoints [16], 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 [17], 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 password may consist of 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.

B. MOBILE AUTHENTICATION

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

Authentication on Apple's iOS operating system is based on four-digit PINs. A 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.

Android's pattern unlock scheme presents a user with a 3×3 grid of dots.[1] Similar to Draw-A-Secret, a user creates a password by drawing lines connecting the dots in a certain way. A valid pattern must consist of at least 4 dots, connected only by straight lines that can be contained inside the grid. The four-digit PIN is also available on Android operating system. Recent versions of the Android operating system rate it higher in security strength than the pattern unlock scheme. Passwords made using this scheme are predictable and prone to hotspots; a small subset of Android unlock patterns are used by a large portion of users [19] and most users tend to use the same heuristic rules to design their passwords [20]. TinyLock [21], a pattern lock scheme, can achieve high usability, but the total number of possible patterns in a 3×3 grid is only 389,112.

The picture authentication scheme developed for Windows 8 allows 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. Microsoft estimates [22] there are roughly 10^9 picture passwords using 3 gestures or less and $6 * 10^{11}$ picture passwords using 4 gestures or less. However, this scheme is vulnerable to dictionary attacks [23], [24] that analyze points of interest in the reference image. For an image with 10 points of interest, there are only about 10^6 combinations for picture passwords of 3 gestures or less and 10^9 combinations for picture passwords with 4 gestures or less [22].

According to our knowledge, this is the first attempt to formally define the concept of multi-facet passwords and analyze their benefits in terms of memory interference, security, and usability. We filed a patent on MAPS in 2013 [25].

C. GAMIFICATION

Gamifying security is an idea that seeks to tie security mechanisms to games in order to improve security, memorability, and usability [26]. For example, the Pass-Go graphical system is based on the board game GO [27]. Hamari *et al.* [28] propose that gamifying an experience can produce positive effects in learning and user experience. Kroeze and Olivier [29] 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.

III. THREAT MODEL

In this paper, we assume the attacker is interested in accessing a mobile device for sensitive data or sensitive applications installed on the mobile device. For example, many services utilize mobile devices as the key to password recovery and the device access allows attackers to compromise these

[1] A larger gird is possible in recent versions of the Android operating system. We focus on the default size of the grid in this paper. Our analysis and conclusion discussed below still holds for larger grids.

services simply by stealing the victim's phone and triggering the password recovery process. 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.

IV. REQUIREMENTS FOR MOBILE AUTHENTICATION

The goal of mobile authentication is to prevent unauthorized access or make the cost of unauthorized access as high as possible. For mobile devices, authentication schemes should satisfy memorability and usability requirements in addition to requirements on security strength. The details of the requirements are presented below:

Security: The scheme should be capable of generating a large amount of possible passwords so that the cost of a brute force attack, in terms of time and effort, can be prohibitive. The security strength of passwords generated with low counts of input gestures is especially important for mobile authentication because of the need for quick access to mobile devices.

Memorability: The passwords generated by the scheme should be easy to remember. However, usually passwords generated by schemes with a larger password space are harder to remember. Another challenge to memorability is *memory interference*, which occurs in human memory when information to store is similar to information previously stored in memory [30]. One example is on alphanumeric passwords, which consist of a string of letters and numbers. Memory interference may occur when a user tries to remember the latter part of a long password, or several passwords for various accounts. This is because each position of an alphanumeric password contains similar information: letters or numbers. Memorability is usually evaluated through user studies.

Usability: Mobile devices are becoming increasingly popular partly because of their usability. Because mobile devices are often used for only moments at a time, it is essential that authentication can be finished easily and quickly. In this paper, we propose a usability metric based on the number of touch gestures required to finish password input on a touch screen of mobile devices. The usability of a mobile authentication scheme can also be measured by the time to finish one authentication. This measure depends on a user's skills of using smartphones and a user's familiarity with an authentication scheme. In addition to the two objective measures described above, the usability can also be measured subjectively with a user survey to ask for users' opinions on the usability of an authentication scheme.

V. MULTI-FACET PASSWORD SCHEME

In this section, we present the design of the Multi-fAcet Password Scheme (MAPS) and use a Chess-based MAPS as an example to explain the rationales behind the design. Then we describe graphical hints designed to improve memorability of MAPS.

A. DESIGN OF MULTI-FACET PASSWORD FOR MOBILE AUTHENTICATION

The key idea of MAPS is to form a password by fusing information from multiple facets. MAPS uses information from multiple facets for two purposes: (1) By using information from multiple facets, a MAPS scheme can generate a large number of possible passwords. (2) Using information from multiple facets can increase the memorability of the password. Alphanumeric passwords are relatively hard to remember partly because of *memory interference*, as introduced in the previous section: Usually an alphanumeric password is made by repeating the same type of information and the repetition may hinder remembering the beginning part of a password when the latter part of the password is being memorized [30]. MAPS can reduce memory interference greatly because information from different facets is not similar to each other. So, MAPS's using information from multiple facets leads to both better security strength and less memory interference.

To further increase MAPS's memorability and usability, we design an information fusion process, which fuses information from multiple facets together. An example explaining the fusion process is described in the next subsection.

We design MAPS as a graphical password for three reasons: (1) Graphical password schemes, which allow users to authenticate themselves by drawing or choosing information based on visual input, are easier to remember than textual password schemes because of the *picture superiority effect* [7]: Psychology researches indicate that humans have tremendous capacity for processing and remembering visual data, far exceeding our ability to process and remember numbers and letters [31], [32]. (2) For mobile devices equipped with touch screens, a graphical password scheme is a natural choice. Typing text passwords on soft keyboards, supported by most current mobile devices, can be relatively slower because of the limited size of the keyboard [33]. In comparison with text password input via soft keyboards, graphical passwords can be easier to input on these devices. (3) Graphical passwords used on touch screens enable fusion of information from multiple facets to increase memorability and usability. More details on the fusion are explained in the next subsection.

To better explain the design of MAPS, we present an example MAPS based on the chess game below.

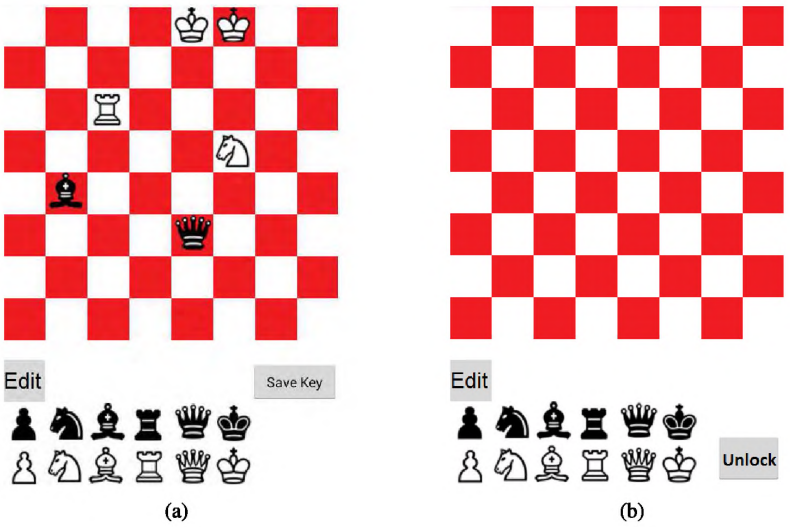


FIGURE 1. Screenshots of a CMAPS implementation. (a) An example CMAPS password. (b) Unlock interface.

B. A CHESS-BASED MAPS (CMAPS)

Figure 1 shows two screenshots of our implementation of Chess-based MAPS (CMAPS) developed for Android systems. A CMAPS user sets a password by placing chess game pieces onto a classical chess game board with 8×8 tiles.[2] The resulting chess formation is a CMAPS password. An example password of CMAPS is shown in Figure 1(a). When the user wants to unlock the mobile device later, CMAPS will display a blank chess board and the chess game pieces as shown in Figure 1(b). 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. The "Edit" button in Figure 1 allows a user to overwrite or empty a game piece on a tile in the chess board.

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.[3] 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.

[2]The size of the chess board in the number of tiles can be adjusted according to screen size. According to Fitts's law [34],[35], user interaction can be slower and less precise when the size of tiles in a board is smaller, especially for smaller screens.

[3]In the paper, we do not include the order in which game pieces are placed onto the board as a part of a CMAPS password. But the order can be included as a part of a CMAPS password and the password space can be further enlarged.

TABLE 1. CMAPS facets.

Facet	Choices
Color	Black or White
Type of Game Pieces	King, Queen, Rook, Bishop, Knight, or pawn
Location of a Game Piece	Row and Column Choice on the Board

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.

C. GRAPHICAL HINTS

To further improve the memorability of MAPS, we ask users to design graphical hints for their MAPS passwords. The graphical hints are kept in the user's memory only: (1) CMAPS cannot store graphical hints generated by users. (2) CMAPS cannot display any graphical hints to a user when the user wants to unlock a device.

For CMAPS, we use the example hints shown in Figure 2 to help users to create their own graphical hints. The example hints are only shown to the participants in our user study for the demo purpose only. Our user study shows that participants generated interesting graphical hints in various ways. More details can be found in Section VII. In Figure 2(a), the game pieces represent American football players arranged on a playing field, with endzones and the 50 yard line marked by black lines. The quarterback, linebackers, receivers, and runningbacks are represented with different game pieces. The quarterback is labeled QB and the linemen are labeled LM.

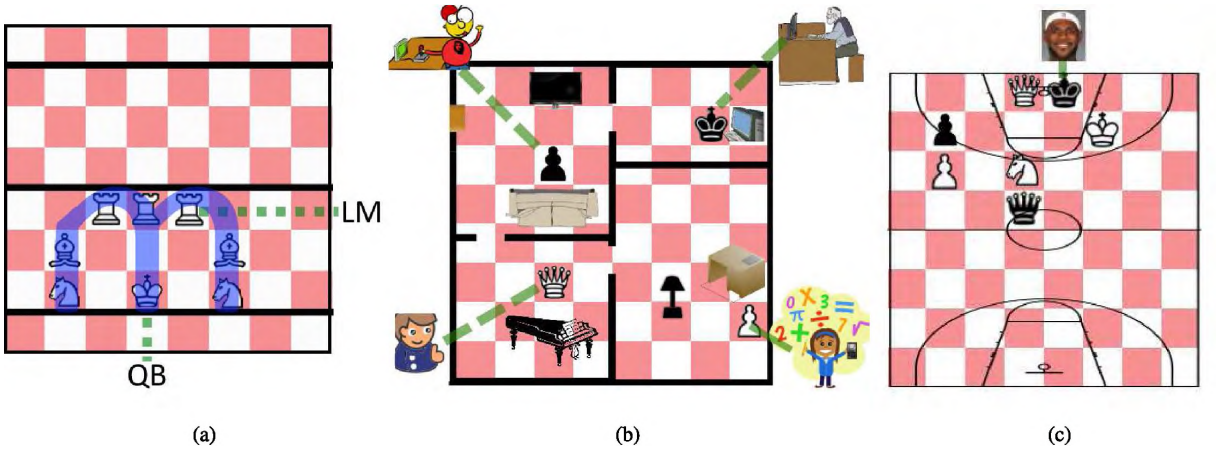


FIGURE 2. Example graphical hints. (a) A football formation. (b) A family in their home. (c) A basketball game.

The hint in Figure 2(b) simulates a family, with the father represented by a black king working on a computer, the mother represented by a white queen playing piano, the older daughter represented by a white pawn doing homework on a desk, and the younger son represented by a black pawn playing video games. In Figure 2(c) the chess formation is used to represent two basketball teams playing on a basketball court. The two teams are in different colors and players in different positions are represented by different types of game pieces.

Unlike pictures in the picture password scheme of Windows 8, graphical hints will not make CMAPS vulnerable to dictionary attacks. Microsoft's picture password is vulnerable to dictionary attacks [24] because the picture used in the scheme is shown for authentication and hot spots in the picture, such as facial features in a face picture, make dictionary attacks feasible. In CMAPS, an authentication always starts with an empty chess board. CMAPS has no knowledge of graphical hints and only users know their own graphical hints.

We hypothesize that graphical hints can reduce the popularity of hotspots, which are defined as frequently selected spots in graphical passwords. Hotspots in graphical passwords enable attackers to launch dictionary attacks [34], which can be significantly more efficient than brute force attacks on graphical password schemes. In CMAPS, if graphical hints are not used, hotspots such as corners or the center of the chess board can be very frequently selected by users for ease of remembering. Similarly certain game pieces can be selected more often than other game pieces. We hypothesize that graphical hints can also reduce the popularity of hotspots in the type of game pieces. More analysis on hotspots in CMAPS is presented in Section VII.

VI. THEORETICAL ANALYSIS

A. SECURITY ANALYSIS

In this subsection, we first measure the security strength of MAPS and then use CMAPS as an example for security analysis. We evaluate the security strength of MAPS and CMAPS with the size of the password space, i.e., the number of possible passwords. The size of password space indicates the probability of obtaining a password through random guess.

1) SECURITY STRENGTH OF MAPS

Assuming the facets in a MAPS are all independent, we can derive the number of possible passwords supported by MAPS as follows.

Proposition 1: For MAPS with n independent facets and m_i possible choices in the ith ($1 \leq i \leq n$) facet, the number of possible passwords having l times of information fusion is $\prod_{i=1}^{n} m_i^l$.

Each information fusion combines choices from all the facets together. So each fusion can have $\prod_{i=1}^{n} m_i$ possible combinations because of the independence. With l times of information fusion, MAPS can generate $\prod_{i=1}^{n} m_i^l$ different passwords.

From Proposition 1, we can derive the following corollary.

Corollary 2: The size of the password space generated by adding t possible choices to one existing facet is no greater than the size of the password space generated by adding one more facet with t possible choices when $t \geq 2$ and the number of existing choices in each facet is greater than or equal to two. Only when $t = 2$ and the facet to add t possible choices has only two possible choices before the addition, the two methods generate password spaces of the same size.

The proof of Corollary 2 is straightforward as adding a facet with t possible choices will enlarge the password space by t^l times where l is the times of information fusion. The proof of Corollary 2 can be found in Appendix A. When t, the number of possible choices to add, is small, the size difference of the password spaces generated by the two methods is not significant. But when t increases, the ratio between the size of the password space generated by adding one more facet of t possible choices and the size of the password space generated by adding t possible choices to an existing facet is $\frac{m_j^l}{(1+\frac{m_j}{t})^l}$ if we assume that the t possible choices are added to the jth facet and m_j denotes the number of possible choices in

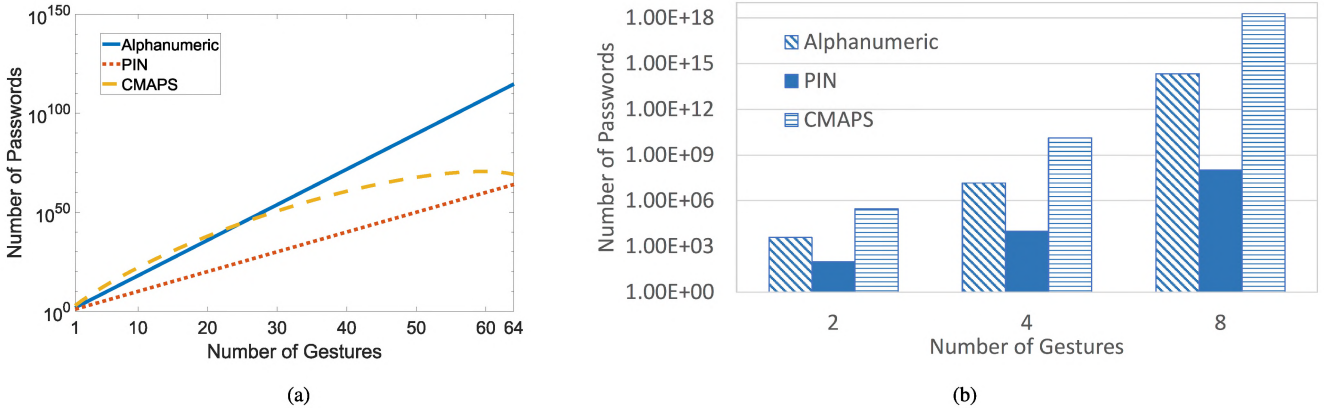


FIGURE 3. Security strength comparison. (a) Number of passwords supported by different number of gestures. (b) Number of passwords supported by two, four, and eight gestures.

the jth facet before the addition. When $t \gg m_j$, the ratio[4] can be approximated as m_j^l, which grows exponentially with l, the times of information fusion. Furthermore, adding more facets and splitting the t possible choices into the added facets can lead to an even larger password space.

Corollary 2 shows the advantage of MAPS over traditional passwords. Traditional passwords such as the alphanumeric passwords and four-digit PINs are essentially one- facet passwords. MAPS, designed to fuse information from multiple facets, can have a significantly larger password space.

2) SECURITY STRENGTH OF CMAPS

In CMAPS, the row and the column are dependent because only one game piece is allowed to be placed in one tile of the chess board.

Proposition 3: With l gestures, CMAPS with the classical chess board of eight rows and eight columns can generate $2^l 6^l \binom{64}{l}$ possible passwords.

The proof of Proposition 3 can be found in Appendix B.

Based on the results in Proposition 3, we compare CMAPS with the PIN-based approach used in Apple's iOS and Google's Android system and the alphanumeric password schemes in terms of the security strength.[5] For fair comparison, we assume that the same number of gestures are used to generate passwords in the password schemes. In iOS, one gesture can select one digit to be used in a passcode. For fair comparison, we assume a PIN can have more than four digits. We assume that one gesture can select one digit or one letter in either the upper case or the lower case to be used in an alphanumeric password, even though for numbers and capital letters an additional gesture may be required to swap to the numeric portion of the soft keyboard or to press the shift key. We do not consider alphanumeric passwords which allow special characters. Similarly, we also assume that in CMAPS, one gesture can put a game piece onto a desired tile in a chess board.

Figure 3, generated based on the assumptions, compares the security strength of the password schemes. From Figure 3(a), we can observe: (1) When the number of gestures is less than 20, CMAPS can generate many more passwords than the PIN-based approach and the alphanumeric password scheme. As most of the alphanumeric passwords used for banking are between eight and 20 characters long, the security strength of CMAPS is higher than the strength required for banking, which is also much higher than the security strength of current mobile authentication schemes such as the PIN-based approach. (2) When the number of gestures is larger than 24, the alphanumeric password scheme can generate more passwords than CMAPS, but CMAPS can still potentially generate about 10^{20} times more passwords than the PIN-based approach. Figure 3(b) shows that two-gesture, four-gesture, and eight-gesture CMAPS passwords can generate about 2900, 1.3×10^6, and 1.9×10^{10} times more passwords than the PIN-based approach respectively and about 75, 890, and 8,700 times more passwords than the alphanumeric password scheme respectively.

B. USABILITY ANALYSIS

In this subsection, 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 [35] as existing graphical password schemes on mobile devices such as the pattern unlock scheme and the picture password scheme. For example, CMAPS does not require a user to carry any additional physical object and the scheme does not require physical user effort beyond gestures on touch screens. In this paper we focus on the ease of

[4]The ratio will increase with t. But adding more facets to share the t possible choices can lead to even larger password space.

[5]We do not include Google's pattern unlock scheme into the comparison because: (1) A pattern used for a pattern unlock can be finished with one long gesture connecting multiple dots in a 3×3 grid. (2) In the security setting menu of the Android operating system, the pattern unlock, PIN, and alphanumeric password are rated as medium security, medium to high security, and high security respectively. We do not include the picture password in Windows 8 because no design details such as the resolution in a circle gesture recognition, i.e., how different two circle gestures can be regarded as the same gesture, are available for the quantitative analysis.

using the password schemes. We evaluate the usability of the schemes with two metrics: the number of gestures required to finish one authentication and the actual time needed to finish one authentication. Both metrics measure the ease of inputting passwords to a mobile device. The difference between the two metrics is that the second measure depends heavily on a user's familiarity with the authentication scheme in a study and a user's skillfulness in using a mobile device.

In this section, we analyze usability with the first metric. The second metric is used in the user study presented in the next section to evaluate usability with timing data collected by the CMAPS application developed for Android smartphones. To obtain direct feedback from users on the usability of CMAPS, we also ask participants of the user study to finish a survey on usability comparison between CMAPS and existing schemes and the survey results are presented in Section VII.

1) NUMBER OF GESTURES REQUIRED TO FINISH A PASSWORD

CMAPS users can place a game piece onto the game board by a gesture drawing a line between a selected game piece and a tile on the chess board. A CMAPS password having l game pieces requires l gestures to input.

TABLE 2. 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

For fair comparison, we assume that passwords generated by all the password schemes are of the same level of security strength.[6] Table 2 shows the comparison results. A user can finish a pattern in the pattern unlock scheme with one long gesture that connects a number of dots in a 3×3 grid. So the gesture connecting multiple dots consists of multiple segments between successive dots. A CMAPS password can also be possibly completed with one gesture connecting multiple games pieces to multiple tiles sequentially, as shown in Appendix C. For fair comparison, Table 2 shows the number of *segments*, i.e. lines connecting two dots, required to finish patterns used in the pattern unlock scheme.

From Table 2, we can observe that CMAPS requires much fewer gestures to achieve similar security strength than other approaches when the size of password space is below 10^{40}. Compared to the pattern unlock scheme and the PIN-based approach, CMAPS requires no more than half the gestures for password spaces between 10^{10} and 10^{30}.

[6]The metric, number of gestures required for a level of password strength, is essentially a reverse way to measure the number of passwords supported by a fixed number of gestures.

VII. USER STUDY

A. OVERVIEW

The goal of the user study is to evaluate the memorability and usability of CMAPS. The study has two sessions. Both sessions are conducted in a controlled laboratory environment to avoid distractions.

During the first session, participants are asked to fill out a consent form with demographical information. They were asked to provide their age range, gender, educational background, skill level of using smartphones, and their chess knowledge. Then we continue with an introduction on CMAPS. Before leaving the laboratory, participants were asked to generate a CMAPS password and recall the password successfully on a smartphone.

To simulate regular use of the passwords as in previous research [36], we sent an email to the participants two days and four days after their first sessions respectively. The emails contain a link to an online emulator of the CMAPS application hosted on Google Sites. The emulator is based on the same code used to generate the application on Android smartphones so the online emulator and the smartphone application have the same user interface and they function in the same way. Participants are encouraged to recall their CMAPS passwords through the online emulator. Use of the emulator is not mandatory because (1) the email response rates may be low and as email communications may not be reliable [37] and (2) we would like to compare password memorability of participants who used the emulator against memorability of those who did not use the emulator to investigate the effect of the daily use of CMAPS passwords.

One week after the first session, participants were invited to return to the controlled laboratory for the second session. Participants were asked to recall their CMAPS passwords through the smartphones that they used in the first session. Participants were allowed to recall their passwords within five minutes. At the end of the second session, participants were asked to fill out a survey rating the usability of CMAPS and their favorite mobile authentication scheme.

B. APPARATUS

An application of CMAPS was implemented and installed on a Samsung Galaxy S4 smartphone configured with the Android Jelly Bean (version 4.2) operating system. The phone is equipped with a 5in Super AMOLED capacitive touchscreen with a 1920×1080 (441 pixels per inch) display resolution. The Android application records attempts made by participants and timing information of each attempt. The implementation does not enforce any rules of chess. Any piece of either color can be positioned on any tile in the chess board, and multiple pieces of the same type are permitted

(e.g. three kings). Only one piece (or no piece) can be placed on any particular tile. Two screen shots of the CMAPS application on Android smartphones are shown in Figure 1.

C. CONDITIONS

To evaluate the memorability and usability of CMAPS passwords with different security strength, we assign participants randomly into the following four conditions: (1) **2g:** CMAPS passwords in this condition must be generated with two gestures. (2) **8g:** CMAPS passwords in this condition must be generated with eight gestures. (3) **8+g:** Participants were asked to generate CMAPS passwords with more than eight gestures. We do not specify a fixed number of gestures in this condition to allow participants to generate CMAPS passwords with as many gestures as they desire. (4) **8+gh:** Before generating CMAPS passwords in this condition, participants were shown graphical hints in Figure 2. The participants assigned into this condition were encouraged to generate their own graphical hints and create their CMAPS passwords based on their own graphical hints. The graphical hints are not stored or displayed in the smartphone application.

D. STATISTICAL TESTING

We use a significance level of 0.05 for our hypothesis testing unless otherwise specified. For omnibus comparisons between categorical and continuous data, we used Chi-squared (χ^2) analysis and Kruskal-Wallis (KW) analysis respectively. If the omnibus test is significant, we perform pairwise tests with Chi-squared for categorical data and Mann-Whitney for quantitative data.

E. PARTICIPANTS

This research was approved by the ethics board of all participating universities. We recruited participants by distributing fliers and leaflet style advertisements. A ten dollar cash incentive was offered for participants who finished both sessions. Sixty-six participants were recruited for the user study and 54 participants finished both sessions. Of the 54 participants who completed the user study, 28 were male and 26 were female. Forty participants were undergraduates, 12 were doctoral or master students, one was staff, and one declined to specify. Twenty eight participants were in engineering majors, 11 were in science majors, and 15 in arts and humanities majors. Twenty six participants were aged between 21 and 25 and 20 were aged 20 and under. Participants were asked "Are you skilled at using Smartphones or mobile devices." On a scale from Strongly Disagree (1) to Strongly Agree (5), participants rated their skill at using smartphones an average of 4.07, with 81% of participants rating their skill 4 or higher.

Among the 66 participants who finished the first session, 12 participants did not return to finish the second session, so the overall dropout rate was 18%. Six of the participants who did not complete the second session indicated a schedule conflict as their reason for failing to attend. The others did not respond to our inquiry after the first session. Of the 12 dropouts, one (8%) was in the 2g condition, two (17%) were in the 8g condition, seven (58%) were in 8+g condition, and two (17%) were in the 8+gh condition. The dropouts did not vary significantly by condition ($\chi^2 = 5.3$, $p = 0.15$). Participant behavior during both sessions was monitored, and participants who appeared distracted had their timing data excluded from analysis. These participants were still compensated as long as they finished both sessions.

F. MEMORABILITY

Table 3 shows the recall rates of CMAPS passwords in each condition after one week. The recall rates are 87% for CMAPS passwords in 8+gh condition and 100% for passwords in the other conditions. The recall results did not vary significantly by condition ($\chi^2 = 5.4$, $p = 0.15$). The results indicate that CMAPS, with security strength exceeding the strength of current mobile authentication schemes and exceeding the requirements of banking, can achieve high recall rates respectively.

TABLE 3. Recall rates of CMAPS passwords.

Conditions	Participants	Recall	Recall Rate
2g	8	8	100%
8g	18	18	100%
$8+g$	13	13	100%
$8+gh$	15	13	87%

To investigate the effect of graphical hints on memorability, we compare results in 8+g and 8+gh conditions. The comparison results indicate that graphical hints did not have significant effect on memorability ($\chi^2 = 1.87$, $p = 0.17$). The results are against our expectation that graphical hints can improve memorability of CMAPS. Our conversations with participants in 8+g condition revealed that many of them already used graphical hints to generate CMAPS passwords without any instruction from us. This fact explains the high recall rate for passwords in 8+g condition. In the user study, participants have created various interesting graphical hints. More details on the graphical hints can be found in the technical report.

We also investigated the effect of using the online emulator between the two sessions on the memorability of CMAPS. To simulate the regular use of passwords, we sent two emails with a link to the online emulator two days and four days after the first session respectively. The majority of participants (87%) responded to at least one email by recalling passwords through the emulator, with 33% responding to both. Only two participants failed to remember their passwords, and both of these participants responded to one email. An omnibus Chi-Squared test on the four conditions (response to both emails, response to the first email only, response to the second email only, and no response) shows no significance ($\chi^2 = 1.68, p = 0.64$). For many users, CMAPS passwords remain memorable after one week without use.

TABLE 4. Pairwise testing on password entry time.

Comparison	Z score	P-value
2g vs 8g	1.70	.09
2g vs 8+g	1.04	.30
2g vs 8+gh	2.36	.01
8g vs 8+g	0.11	.91
8g vs 8+gh	-1.77	.08
8+g vs 8+gh	-2.03	.04

TABLE 5. Average usability rating of CMAPS and other schemes.

Scheme	Ratings	Convenience	Speed
CMAPS-2g	8	4.5	3.88
CMAPS-8g	18	4	3.61
CMAPS-8+g	13	4.08	3.54
CMAPS-8+gh	15	3.67	3.6
4-digit PIN	29	4.48	4.52
Google Pattern	7	4	4.29
Fingerprint	11	4.46	4.64

G. USABILITY

We evaluate the usability of CMAPS with timing data collected by the smartphone application and survey data collected through the usability survey.

1) PASSWORD ENTRY TIME

The smartphone application records timing information of each authentication attempt. Participants had only one authentication session each, and were not permitted to practice beforehand. Only timing data from participants whom we observed to be distracted during the second session was excluded. Examples of distraction include dropping the device or accidentally closing/minimizing the application. The attempts were excluded because allowing those participants another attempt would give them an unfair advantage. Roughly 5% of the data was omitted in this manner. The recall rates are calculated with the distracted participants included.

We examined the total authentication time, including unsuccessful attempts and time that users spent on thinking between attempts. Participants required a mean of 10, 21, 23, and 25 seconds to authenticate themselves in the 2g, 8g, 8+g, and 8+gh conditions respectively. A Kruskal-Wallis test using the timing data from the four conditions (2g, 8g, 8+g, and 8+gh) indicates significance ($H = 10.998, p < 0.012$). Pairwise Mann-Whitney comparisons between the categories show significant differences between 2g and 8g ($Z = 2.69, p = .007$), and between 2g and 8+gh ($Z = 3.01$, $p = .002$). Despite 8+g being slower than both 2g and 8g on average, there was no significant difference between 2g and 8+g ($Z = 1.27, p = .20$). We attribute this result to 3 exceptionally fast outliers in 8+g who required 10 seconds or less to authenticate themselves. The fastest 70% of users in each condition authenticated in a mean of 9, 14, 11, and 19 seconds respectively.

The total password entry time for a CMAPS password is comparable to other graphical schemes such as Deja Vu (31-36s) [11], CDS (20s) [38], Story (23s) [38], and Draw a Secret (5-12s) [39].[7]

We also examined the time spent on only the first successful attempt. The time is calculated as time from when the screen with the board loads to first correct authentication, or from previous unsuccessful authentication to successful authentication. Participants required a mean of 10, 14, 14, and 20 seconds for the first successful authentication attempt in the 2g, 8g, 8+g, and 8+gh conditions respectively. As expected, authentication time increases with the number of gestures. A Kruskal-Wallis test using the timing data from the four conditions indicates significance ($H = 8.08, p < 0.044$). Table 4 shows pairwise comparisons with the two tailed Mann-Whitney test. Both 2g and 8+g show significance with 8+gh, however 8g does not, which we attribute to a small number of fast outliers in 8g. We attribute the lack of significance between 8+g and 8g to users in 8+g opting to use as few pieces as possible.

The password entry time for one entry of a CMAPS password is comparable to other schemes such as CDS (14s), Story (9s), Xside (3-4s) [15], SwiPIN (4-5s) [18], and TinyLock (2-4s) [21]. We note that 4 gesture CMAPS can generate 1.3×10^6 times more passwords than 4-digit PIN or SwiPin, and 33,859 times more passwords than the total number of possible passwords in Android's pattern unlock or TinyLock with a 3×3 grid.

The average number of attempts required to authenticate also increases with the number of gestures. Participants in 2g, 8g, 8+g, and 8+gh required 1, 1.3, 1.4, and 1.4 attempts for each condition respectively. A Kruskal-Wallis test on the attempts required shows no significance ($H = 1.144, p = 0.767$).

We did not conduct a user study on existing mobile authentication schemes to compare CMAPS against existing mobile authentication schemes on the password entry time and memorability because the comparison will be biased. Existing schemes such as the pattern unlock scheme and the four-digit PIN are already being used by the participants. So the participants may simply reuse their current passwords in the user study. Even if the participants did not use their current passwords, their familiarity with the existing schemes causes bias in the comparison as they only used CMAPS for a couple of times and the existing schemes are being used daily. So we conduct a usability survey to compare CMAPS against the existing schemes.

2) USABILITY SURVEY

Participants finish a usability survey at the end of the second session. In the survey, we asked participants whether they agreed with the following statements: (1) the authentication scheme is convenient, and (2) entering a password with the authentication scheme is fast. Participants rate CMAPS in their condition (2g, 8g, 8+g, or 8+gh), and

[7] Deja Vu, CDS, and Story use a mouse for input. Draw a Secret is based on a touch screen.

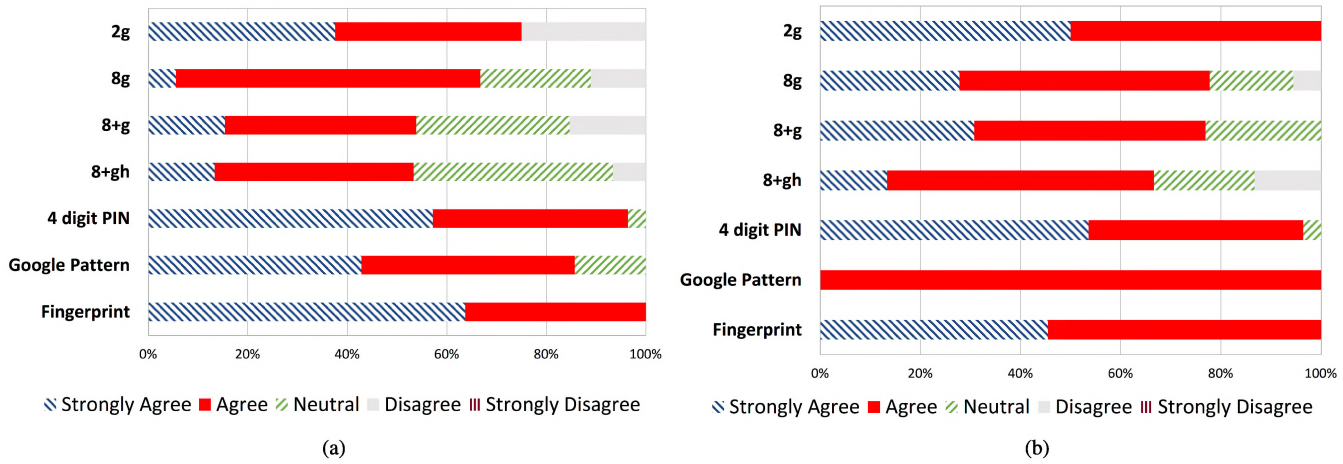


FIGURE 4. Survey results. (a) Entering password convenient. (b) Entering password fast.

whichever authentication scheme is currently used by the participant, or their favorite scheme if they do not currently use any kind of authentication. The possible choices are strongly disagree, disagree, neutral, agree, and strongly agree. For quantitative analysis, the choices are converted to 1 (strongly disagree) to 5 (strongly agree). Figure 4 shows the survey results and the average usability rating results are shown in Table 5.

Responses from the survey were further sorted as either *unsatisfactory* (1-3) or satisfactory (4,5). Table 6 shows that CMAPS has no significant difference in usability among the four conditions (2g, 8g, 8+g, and 8+gh).

TABLE 6. Statistical analysis on usability data for CMAPS.

	Convenience		Speed	
	χ^2	p	χ^2	p
Omnibus	3.36	.399	2.56	.465
Category	**Pairwise Test Result**			
2g vs 8g	2.10	.147	.181	.671
2g vs 8+g	2.15	.142	.940	.332
2g vs 8+gh	3.41	.065	1.02	.310
8g vs 8+g	.003	.955	.523	.470
8g vs 8+gh	3.41	.065	.609	.465
8+g vs 8+gh	.509	.476	.068	.795

We further compared CMAPS with authentication schemes in use by the participants. Since each participant is only asked about CMAPS and the authentication scheme in use, only pairwise testing is used for analysis. Table 7 shows our results. Not included in the table are the five participants who never used another mobile security scheme, the only one participant who chose facial recognition, and the only one who chose the windows picture password. In terms of convenience, participants felt that CMAPS in 8g was not significantly different from the four-digit PIN, the pattern unlock scheme, and the fingerprint scheme. CMAPS in 8+g and 8+gh were rated as significantly less convenient than the four-digit PIN. In terms of input speed, CMAPS with more than two gestures was rated lower than the four-digit PIN and fingerprint, but was not significantly different from the pattern unlock scheme.

TABLE 7. Statistical Analysis Comparing CMAPS to Other Schemes. (CMAPS results are sorted by gesture. Other schemes are abbreviated for brevity. PIN: four-digit PIN, Patt: Google's pattern unlock, print: fingerprint scheme. Two categories could not be tested because they had perfect ratings. Significant p values are bolded for visibility.)

	Convenience		Speed	
	χ^2	p	χ^2	p
2g vs PIN	.284	.594	.284	.594
8g vs PIN	.198	.656	**7.83**	**.005**
8+g vs PIN	**4.01**	**.045**	**11.8**	**.001**
8+gh vs PIN	**7.50**	**.006**	**12.4**	**.001**
2g vs Patt	NA	NA	.268	.605
8g vs Patt	1.85	.174	.907	.341
8+g vs Patt	.359	.549	2.03	.154
8+gh vs Patt	3.02	.082	2.16	.141
2g vs print	NA	NA	3.07	.080
8g vs print	2.84	.092	**4.62**	**.032**
8+g vs print	2.90	.089	**6.77**	**.009**
8+gh vs print	2.90	.089	**7.02**	**.008**

The convenience results in Table 4 indicate that user satisfaction to CMAPS in 2g and 8g is at the same level as the user satisfaction to four-digit PIN. The results also show that user satisfaction to CMAPS in 8g, 8+g, and 8+gh is at the same level as user satisfaction to pattern unlock.

From the survey data, we can conclude that CMAPS in 2g, with security strength exceeding the strength of current mobile authentication schemes, can be used as an acceptable alternative to existing authentication schemes such as the four-digit PIN in terms of usability. We can also observe that CMAPS in 8g, with security strength exceeding the requirements of banking, is comparable with current mobile authentication schemes in terms of usability.

H. HOTSPOTS

Hotspots, defined as frequently selected spots in graphical passwords [34], enable attackers to launch efficient

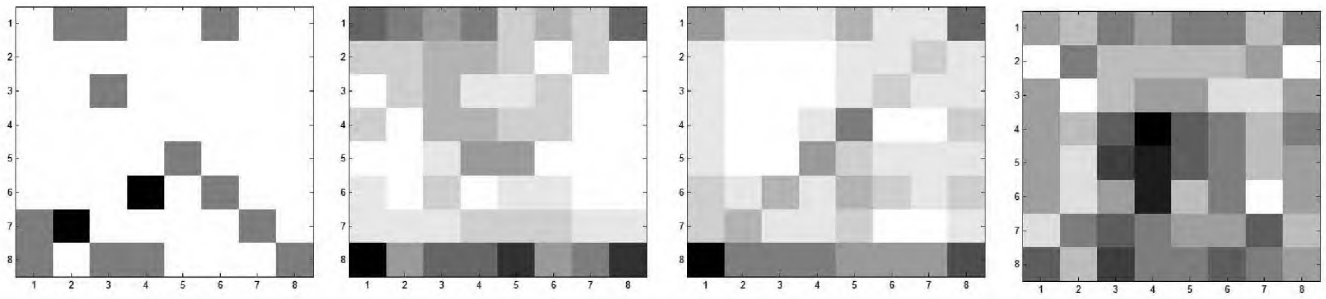


FIGURE 5. Popularity of Tiles (The gray level of each tile indicates the popularity of each tile. The most popular tile and the least popular tiles are in the color black and the color white respectively.) From left to right: 2 piece, 8 piece, unlimited (8+) pieces, unlimited (8+) pieces with hints.

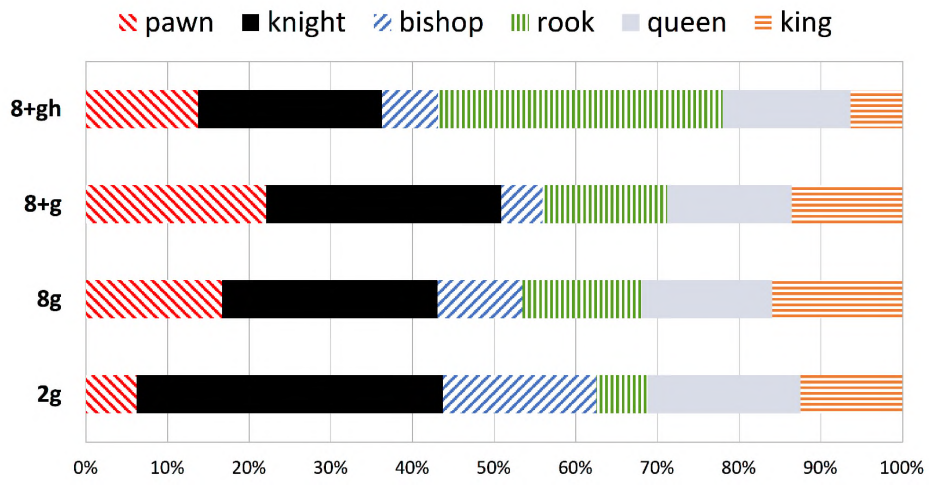


FIGURE 6. Popularity of different piece types.

attacks such as the dictionary attack. Hotspots reduce uncertainty in password choices. Graphical schemes that depend on pictures or images can be vulnerable to hotspots [40]. In this paper we evaluate the hotspot effect with Shannon's entropy [41], an information-theoretical measure of uncertainty. The entropy E is defined as follows:

$$E = -\sum_{i} p_i \log_2 p_i \tag{1}$$

where p_i denotes the probability of selecting the ith choice. In CMAPS, the hotspot effect may exist in the choices on the tiles of the chess board and in the choices on the type of game pieces.

1) HOTSPOTS IN TILE SELECTION

Figure 5 shows popularity of tiles. We can observe that some tiles, particularly the corner tiles, were chosen more often than others. Assuming a uniform distribution on the tile selection, we can calculate entropy $E^{tile}_{uniform} = 6.00$ bits according to the entropy defined in Equation 1 as $p_i = \frac{1}{64}$, $1 \le i \le 64$. Similarly we can calculate the entropy E^{tile}_{C}, denoted as the entropy of tile selection in Condition C. According to the popularity shown in Figure 5, E^{tile}_{2g}, E^{tile}_{8g}, E^{tile}_{8+g}, and E^{tile}_{8+gh} are 3.75, 5.25, 5.26, and 5.76 bits respectively. So the hotspots in tile selection reduce the uncertainty by 2.25, 0.75, 0.74, and 0.24 bits in 2g, 8g, 8+g, and 8+gh conditions respectively. The reduction in uncertainty, i.e., the popularity of hotspots decreases as the number of gestures increases since more tiles are to be used. The data also shows that graphical hints can reduce popularity of hotspots when we compare the entropy of 8+g with the entropy of 8+gh. Overall the entropy of 8g, 8+g, and 8+gh conditions are very close to the maximum entropy of 6.00 bits. The results indicate that when the number of gestures is larger than eight, the hotspot effect can be largely ignored as the popularity of each tile is about the same.

2) HOTSPOTS IN PIECE SELECTION

Figure 6 shows the distribution of piece types. Ideally each piece will be selected 100/6 = 17% of the time. Our data shows that pawns, rooks, queens, and kings were placed 18%, 14%, 16%, and 15% of the time respectively. Knights were placed 28% of the time, while bishops were placed only 9% of the time.

Assuming a uniform distribution on the selection of the piece type, we can calculate entropy of piece type $E^{type}_{uniform} = 2.59$ bits according to the entropy definition

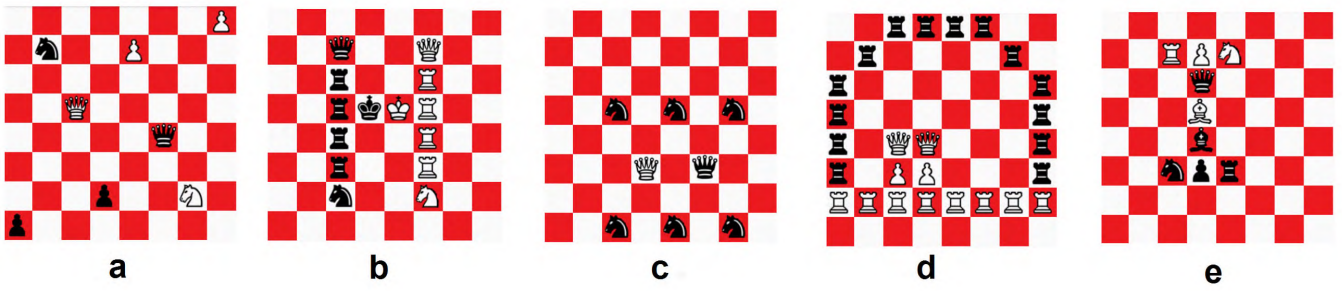


FIGURE 7. Example graphical hints created by users.

in (1) as $p_i = \frac{1}{6}$, $1 \leq i \leq 6$. Similarly we can calculate the entropy E_C^{type}, denoted as the entropy of piece type selection in Condition C. According to the popularity shown in Figure 6, E_{2g}^{type}, E_{8g}^{type}, E_{8+g}^{type}, and E_{8+gh}^{type} are 2.31, 2.52, 2.44, and 2.34 bits respectively. The results show the number of gestures does not have a predictable effect on hotspots in piece type. We can also observe that the entropy of each condition is very close to the maximum entropy of 2.59 bits. It indicates that the hotspot effect can be largely ignored.

I. GRAPHICAL HINTS CREATED BY PARTICIPANTS

Users in the 8+gh condition used an average of 13.6 pieces with a median of 12. Only 20% of users in this category chose to use 8 pieces exactly.

At the end of the experiment, we asked some 8+gh participants to describe their graphical hints. Some user generated hints are presented here. Figure 7 shows some example graphical hints created by participants. Password (a) is based on chess. The knights are used as a reference. Each knight is attacking a queen, which is covering a pawn. A pawn of the queen's color sits in the corner. Password (b) is the letter H, with colors swapped between the two sides. The bulk of the vertical lines are made up of rooks, but the top and bottom of each line is capped with a unique piece, and the horizontal center line is made from kings.Password (c) represents a casino floor. The play tables are on red tiles, denoted with knights. Pit bosses, denoted as queens, watch the tables from the white tiles between them. Password (d) is a house. The floor or foundation is built from white rooks, and the remainder from black rooks. Two women, their bodies made of pawns and their heads made of queens, sit inside the house. Password (e) is a cricket field, with different pieces denoting different players around the two wickets. The queen is the user's favorite player.

VIII. DISCUSSION

In this section, we discuss the impact of chess knowledge to the memorability of CMAPS and an extension of CMAPS to reduce or even eliminate side effects of password expiration policies.

A. IMPACT OF CHESS KNOWLEDGE

Participants indicated whether or not they could play chess by answering yes or no in the consent form. Ignoring the participants who did not answer, 81% answered yes, 19% answered no. Only two users forgot their passwords, one that knew how to play chess and one that did not. Thus we find that chess knowledge does not have significant impact on remembering the password ($\chi^2 = .26$, $p = 0.61$), and it means that CMAPS passwords are memorable even to people with no knowledge of chess.

B. EXTENSION

To foil an attacker who obtains the older password through various possible ways such as brute force attacks, interception, or simply guessing, system owners or administrators prefer expiring old passwords every few months or weeks and asking system users to generate new passwords. While the password expiration policies can possibly help secure the system by reducing the time that an attacker has to access the system, the password expiration policies can cause extra burden on system users such as interruption of ongoing work and increase in login errors. Zhang *et al.* [42] even reported that the knowledge of old passwords can help in breaking new passwords.

MAPS can be extended to reduce or eliminate the side effects of the password expiration policies. The extension is to add a game facet to MAPS. In other words, when a user is required to change an old password based on one game, the user can select another game and form a new password based on the new game. To better reduce or eliminate side effects, the systems may use games that are as different as possible. For example, if the old password is based on chess, the system may suggest the user to use the game Monopoly for the new password.

The game change can help reduce memory interference in long term memory, which is used for continuing storage of information [30], as the new game is completely different from the old game and the passwords formed based on the different games are less likely to cause memory interference.

The addition of the game facet can also prevent breaking new passwords based on the knowledge of old passwords. MAPS based on different games may have different sets of

facets so no connection between new passwords and old passwords is available. For example games chess and Monopoly have different sets of game pieces/rules and completely different game boards.

We plan to perform a user study on the extension in our future work. Since passwords usually expire every 3 months or 6 months, the user study may take a long time.

IX. 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 of 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.

APPENDIX A
PROOF OF PASSWORD SPACE OF MAPS

Proof: First the number of existing choices in each facet has to be greater than or equal to two. If there is only one possible choice in one facet, the facet can be removed and the size of the password space will not change. So if we denote the number of possible choices in the jth facet as m_j, $m_j \geq 2$. Without loss of generality, we assume the t possible choices are added to the jth facet, so the size of the password space generated by adding the t possible choices, denoted as S_1, can be derived according to Proposition 1 as follows:

$$S_1 = (\prod_{i=1}^{j-1} m_i^l)(m_j + t)^l(\prod_{i=j+1}^{n} m_i^l) \tag{2}$$

where n denotes the number of existing facets and l denotes the times of information fusion. The size of the password space generated by adding one more facet of t choices, denoted as S_2, can be derived according to Proposition 1 as follows:

$$S_2 = (\prod_{i=1}^{j-1} m_i^l)m_j^l(\prod_{i=j+1}^{n} m_i^l)t^l \tag{3}$$

where n denotes the number of existing facets and l denotes the times of information fusion. Since $t \geq 2$ and $m_j \geq 2$, we can derive

$$(t-1)(m_j - 1) \geq 1. \tag{4}$$

After simplification on Inequality 4, we can derive

$$tm_j \geq t + m_j. \tag{5}$$

Combining Equation 2 and Inequality 5, we can derive as follows:

$$\begin{aligned} S_1 &\leq (\prod_{i=1}^{j-1} m_i^l)m_j^l t^l(\prod_{i=j+1}^{n} m_i^l) \\ &= S_2 \end{aligned} \tag{6}$$

We have equality in 4, only if $t = 2$ and $m_j = 2$. So the two methods generate password space of the same size only when $t = 2$ and $m_j = 2$. □

APPENDIX B
PROOF OF PASSWORD SPACE OF CMAPS

Proof: According to the description of CMAPS in Section V-A, one gesture can select one game piece and put the game piece onto the game board. So one gesture in CMAPS is equivalent to one time of information fusion in MAPS. The process of generating one l-gesture CMAPS password can be equivalently divided into three phases: (1) In the first phase, l game pieces are selected in order. (2) In the second phase, l tiles on the chess board are selected. (3) In the third phase, the selected l game pieces are put onto the selected l tiles one by one according to the piece selection order.

In the first phase, the number of possible permutations of l game pieces is $2^l 6^l$ because there are two colors and six types of game pieces available for choices and the color facet is independent from the facet of the piece type. We calculate the number of possible permutations of l game pieces instead of combination of l game pieces to remove duplicate passwords generated because of different orders of putting game pieces onto a game board. For example, one CMAPS password with two white kings on two selected tiles can be created in two different ways dependent on which king is first put onto the board. But actually, the two passwords created in different ways are identical. Even for different types of games pieces, different orders of placing selected game pieces onto a game board can generate duplicate passwords. So to remove the duplicates caused by different orders, we calculate the permutation of l game pieces to be put onto the board. The permutation can remove duplicates because only *one* order of placing the selected l game pieces onto their corresponding tiles is counted in a permutation. We use corresponding tiles in the previous sentence to emphasize that the selected pieces will be put into selected tiles in the piece selection order.

In the second phase, l tiles are selected for the selected l game pieces. Totally there are 64 tiles in the classical 8×8 chess board. So the number of possible combinations of l selected tiles is $\binom{64}{l}$.

In the third phase, the l selected game pieces are put onto the l selected tiles according to the piece selection order. A selected tile is assigned to a selected game piece as follows: (1) The selected tiles are ordered according to their row numbers and column numbers in the chess board. The tile in the ath row and bth column is labeled as the $[(a-1) * 8 + b]$th tile. (2) The l selected tiles are ordered in a queue according to their labels. (3) Each game piece

will be assigned to a tile that has the same position in the queue as the game piece's position in the permutation. For each permutation of l game pieces, there are $\binom{64}{l}$ different passwords. Given $2^l 6^l$ permutations, one l-gesture CMAPS can generate $2^l 6^l \binom{64}{l}$ possible passwords.

Because of the removal of duplicates in the first phase and the arrangement in the third phase, the piece selection and the piece placement are independent. So in the final step of the derivation, we can use multiplication to obtain the number of possible passwords. □

APPENDIX C
AN IMPLEMENTATION OF A SINGLE-GESTURE CMAPS

Figure 8 shows the possibility of finishing one CMAPS password with one long gesture. In our future work, we will investigate whether users will actually use one gesture to finish CMAPS passwords. The popularity of the pattern unlock on Android systems shows users' preference on authentication with one long gesture.

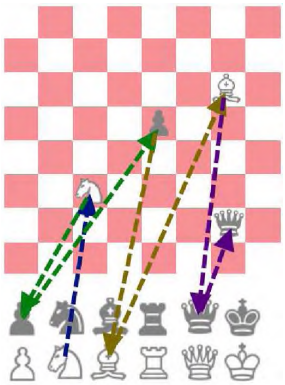


FIGURE 8. One Gesture that completes a cmaps password of four game pieces (The gesture starts from the white knight. For visual clarity, we use different colors to draw segments to place different game pieces.)

REFERENCES

[1] T. Hornyak. (Jan. 2014). *1 Billion Smartphones Shipped Worldwide in 2013*. [Online]. Available: http://www.pcworld.com/article/2091940/global-smartphone-shipments-topped-1-billion-in-2013.html

[2] C. Herley and P. C. van Oorschot, "A research agenda acknowledging the persistence of passwords," *IEEE Security Privacy*, vol. 10, no. 1, pp. 28–36, Jan. 2012.

[3] B. Chaparro, B. Nguyen, M. Phan, A. Smith, and J. Teyes, "Keyboard performance: Ipad versus netbook," *Usablity News*, vol. 12, no. 2, Nov. 2010.

[4] M. D. H. Abdullah, A. H. Abdullah, N. Ithnin, and H. K. Mammi, "Towards identifying usability and security features of graphical password in knowledge based authentication technique," in *Proc. 2nd Asia Int. Conf. Model. Simul.*, May 2008, pp. 396–403.

[5] G. E. Blonder, "Graphical password," U.S. Patent 5 559 961 A, Sep. 24, 1996.

[6] 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.

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

[8] 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. 1789–1794.

[9] R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Comput. Surv.*, vol. 44, no. 4, 2012, Art. no. 19.

[10] J. G. W. Raaijmakers and R. M. Shiffrin, "Models for recall and recognition," *Annu. Rev. Psychol.*, vol. 43, pp. 205–234, Feb. 1992.

[11] R. Dhamija and A. Perrig, "Deja Vu—A user study: Using images for authentication," in *Proc. 9th Conf. USENIX Secur. Symp.*, vol. 9, 2000, p. 4.

[12] RealUser. *Passfaces: Two Factor Authentication for the Enterprise*. [Online]. Available: http://www.realuser.com

[13] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in *Proc. 13th Conf. USENIX Secur. Symp.*, vol. 13, 2004, p. 11.

[14] J. Nicholson, L. Coventry, and P. Briggs, "Age-related performance issues for PIN and face-based authentication systems," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, 2013, pp. 323–332.

[15] A. De Luca *et al.*, "Now you see me, now you don't: Protecting smartphone authentication from shoulder surfers," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, 2014, pp. 2937–2946.

[16] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *Int. J. Human-Comput. Stud.*, vol. 63, nos. 1–2, pp. 102–127, Jul. 2005.

[17] W. A. J. van Eekelen, J. van den Elst, and V.-J. Khan, "Picassopass: A password scheme using a dynamically layered combination of graphical elements," in *Proc. Extended Abstr. Hum. Factors Comput. Syst. (CHI)*, 2013, pp. 1857–1862.

[18] E. von Zezschwitz, A. De Luca, B. Brunkow, and H. Hussmann, "SwiPIN: Fast and secure PIN-entry on smartphones," in *Proc. ACM Conf. Hum. Factors Comput. Syst.*, 2015, pp. 1403–1406.

[19] S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz, "Quantifying the security of graphical passwords: The case of android unlock patterns," in *Proc. SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 161–172.

[20] P. Andriotis, T. Tryfonas, and G. Oikonomou, "Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method," in *Proc. Int. Conf. Hum. Aspects Inf. Secur., Privacy, Trust*, 2014, pp. 115–126.

[21] T. Kwon and S. Na, "TinyLock: Affordable defense against smudge attacks on smartphone pattern lock systems," *Comput. Secur.*, vol. 42, pp. 137–150, May 2014.

[22] S. Sinofsky. *Signing in With a Picture Password*. [Online]. Available: http://blogs.msdn.com/b/b8/archive/2011/12/16/signing-in-with-a-picture-password.aspx

[23] A. Sadovnik and T. Chen, "A visual dictionary attack on picture passwords," in *Proc. IEEE Int. Conf. Image Process.*, Sep. 2013, pp. 4447–4451.

[24] Z. Zhao, G.-J. Ahn, J. Seo, and H. Hu, "On the security of picture gesture authentication," in *Proc. USENIX Conf. Sec.*, 2013, pp. 383–398.

[25] 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.

[26] S. Deterding, M. Sicart, L. Nacke, K. O'Hara, and D. Dixon, "Gamification. Using game-design elements in non-gaming contexts," in *Proc. Extended Abstr. Hum. Factors Comput. Syst. (CHI)*, 2011, pp. 2425–2428.

[27] H. Tao, "Pass-go, a new graphical password scheme," M.S. thesis, Univ. Ottawa, Ottawa, On, Canada, 2006.

[28] J. Hamari, J. Koivisto, and H. Sarsa, "Does gamification work?—A literature review of empirical studies on gamification," in *Proc. IEEE 47th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2014, pp. 3025–3034.

[29] C. Kroeze and M. S. Olivier, "Gamifying authentication," in *Proc. IEEE Inf. Secur. South Africa (ISSA)*, Aug. 2012, pp. 1–8.

[30] A. L. Titcomb, V. F. Reyna, F. N. Dempster, and C. J. Brainerd, "Memory interference and misinformation effects," in *Interference and Inhibition in Cognition*, 1995, pp. 263–294.

[31] R. N. Shepard, "Recognition memory for words, sentences, and pictures," *J. Verbal Learn. Verbal Behavior*, vol. 6, no. 1, pp. 156–163, 1967.

[32] R. S. Nickerson, "Short-term memory for complex meaningful visual configurations: A demonstration of capacity," *Can. J. Psychol.*, vol. 19, no. 2, pp. 155–160, 1964.

[33] I. S. MacKenzie, S. X. Zhang, and R. W. Soukoreff, "Text entry using soft keyboards," *Behav. Inf. Technol.*, vol. 18, no. 4, pp. 235–244, 1999.

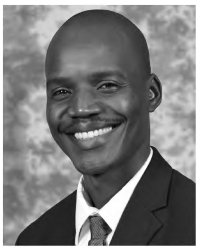
[34] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot-spots in graphical passwords," in *Proc. 16th Conf. USENIX Sec. Symp.*, 2007, pp. 103–118.

[35] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes," in *Proc. IEEE Symp. Secur. Privacy*, May 2012, pp. 553–567.
[36] N. Wright, A. S. Patrick, and R. Biddle, "Do you see your password?: Applying recognition to textual passwords," in *Proc. 8th Symp. Usable Privacy Secur.*, 2012, Art. no. 8.
[37] N. Hikmet and S. K. Chen, "An investigation into low mail survey response rates of information technology users in health care organizations," *Int. J. Med. Inform.*, vol. 72, nos. 1–3, pp. 29–34, 2003.
[38] H. Gao, Z. Ren, X. Chang, X. Liu, and U. Aickelin, "A new graphical password scheme resistant to shoulder-surfing," in *Proc. Int. Conf. Cyberworlds*, Oct. 2010, pp. 194–199.
[39] N. H. Zakaria, D. Griffiths, S. Brostoff, and J. Yan, "Shoulder surfing defence for recall-based graphical passwords," in *Proc. 7th Symp. Usable Privacy Secur.*, 2011, Art. no. 6.
[40] F. Alt, S. Schneegass, A. S. Shirazi, M. Hassib, and A. Bulling, "Graphical passwords in the wild: Understanding how users choose pictures and passwords in image-based authentication schemes," in *Proc. 17th Int. Conf. Hum.-Comput. Interact. Mobile Devices Services*, 2015, pp. 316–322.
[41] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 1991.
[42] Y. Zhang, F. Monrose, and M. K. Reiter, "The security of modern password expiration: an algorithmic framework and empirical analysis," in *Proc. 17th ACM Conf. Comput. Commun. Secur.*, 2010, pp. 176–186.

YE ZHU received the B.Sc. degree from Shanghai Jiao Tong University, the M.Sc. degree from Texas A&M University, and the Ph.D. degree from the Electrical and Computer Engineering Department, Texas A&M University. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, Cleveland State University. His research interests include usable security, mobile computing, peer-to-peer networking, and traffic engineering. He is a member of the IEEE Computer Society. His research results are published in prestigious conferences and journals, such as ACM TISSEC and IEEE TPDS.

JONATHAN GURARY received the B.S. degree in computer engineering, the M.S. degree in electrical engineering, and the Ph.D. degree in computer engineering from Cleveland State University. He is currently a Visiting Professor at John Carroll University. His research interests are in human–computer interaction with cybersecurity systems, usable security, mobile device authentication, and security inside virtual and augmented realities.

GEORGE CORSER (M'11) received the bachelor's degree in civil engineering from Princeton University, Princeton, NJ, USA, the master's degree in computer and information sciences from the University of Michigan–Flint, Flint, MI, USA, and the Ph.D. degree in computer science and informatics from Oakland University, Rochester, MI, USA. He serves as an Assistant Professor of computer science and information systems at Saginaw Valley State University, University Center, MI, USA, where he teaches coursework focusing on mobile app and web app development. His current research focuses on mobile and IoT cyber security, especially vehicular ad hoc network security and location privacy.



JARED OLUOCH received the M.Sc. degree in management information systems from the University of Nebraska at Omaha in 2009, and the Ph.D. degree in computer science and informatics from Oakland University, Rochester, MI, USA, in 2015.

He is currently an Assistant Professor of computer science and engineering technology with the Department of Engineering Technology, University of Toledo. His research interests are in trust management and reputation of connected vehicles; information security; localization for wireless sensor networks and physical layer security.

NAHED ALNAHASH received the B.S. degree in computer science (a minor in mathematics) from Pittsburg State University, Pittsburg, KS, USA, and the M.S. degree in computer science from Texas A&M University at Commerce, TX, USA. She is currently pursuing the Ph.D. degree in computer science and informatics at Oakland University, Rochester, MI, USA. Her research interests are network security, mobile security, and communication systems. Her recent research focuses on wireless sensor networks, especially water monitoring systems.

HUIRONG FU (M'01) received the Ph.D. degree from Nanyang Technological University, Singapore, in 2000. She joined Oakland University, Rochester, MI, USA, as an Assistant Professor in 2005, where she is currently a Professor with the Department of Computer Science and Engineering. Previously, she was an Assistant Professor with North Dakota State University, Fargo, for three years, and a Post-Doctoral Research Associate with Rice University, Houston, TX, USA, for two years. As a Lead Professor and the Principal Investigator for several projects funded by the National Science Foundation, she has been actively conducting research in the areas of networks, security, and privacy.

JUNHUA TANG received the B.Eng. and Ph.D. degrees from Shanghai Jiao Tong University, China, in 1994 and 1999, respectively. From 1999 to 2000, she was a Research Fellow at Nanyang Technological University, Singapore. From 2000 to 2001, she was a Technical Consultant with Lucent Technologies Singapore. From 2002 to 2007, she was a Teaching Fellow then an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. Since 2006, she has been with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, where she is currently an Associate Professor. Her research interests include wireless communication and network security.