MAPS: A Multi-Dimensional Password Scheme for Mobile Authentication

Jonathan Gurary
Cleveland State University
j.gurary@vikes.csuohio.edu

Jared Oluoch
Oakland University
jooluoch@oakland.edu

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

Nahed Alnahash
Oakland University
nalnahas@oakland.edu

George Corser
Oakland University
gpcorser@oakland.edu

Huirong Fu
Oakland University
fu@oakland.edu

ITS 2015, November 15–18, 2015, Funchal/Madeira, Portugal.
ACM 978-1-4503-3899-8/15/11.
http://dx.doi.org/10.1145/2817721.2823479

Abstract
It has been long recognized that no silver bullet exists to achieve both *security* and *memorability*. With the addition of *usability requirements*, the task of designing authentication schemes for mobile devices becomes more challenging. We propose a Multi-dimensionAl Password Scheme (MAPS) for mobile authentication. MAPS fuses information from multiple dimensions to form a password. This fusion enlarges the password space, improves memorability, and enhances usability by reducing the number of gestures needed for authentication. Based on the idea of MAPS, we implement a Chess-based MAPS (CMAPS) for Android systems. Our user studies show that CMAPS can achieve high recall rates while exceeding the security strength of current mobile authentication schemes and exceeding the requirements of banking.

Author Keywords
Shoulder-Surfing, Challenge-Response, Graphical Password, Mobile Security, Multidimensional Password

Introduction
We propose a Multi-DimensionAl Password Scheme (MAPS) for mobile authentication. Because MAPS combines information from multiple dimensions, i.e. different types of information, to generate passwords, MAPS can generate a huge number of passwords with

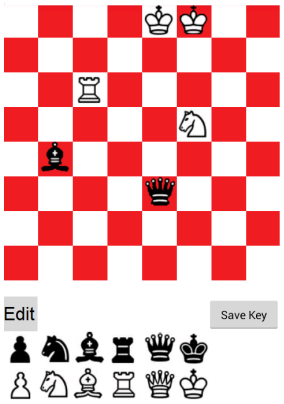

Figure 1: An Example CMAPS Password

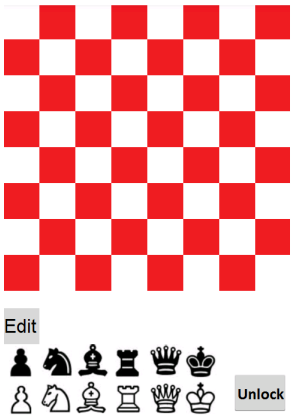

Figure 2: User Interface

just a small number of gestures. Passwords generated by MAPS are easy to remember because (1) MAPS is a type of graphical authentication scheme, which have been proven easier to remember than alphanumeric passwords [8], (2) MAPS fuses information from multiple dimensions through a single gesture on a touch screen, and (3) MAPS can reduce memory interference since the information is from different dimensions. MAPS is also easy to use on mobile devices with touch screens since passwords generated by MAPS can be input with significantly fewer gestures.

In this paper, we present Chess-based MAPS (CMAPS), a mobile authentication based on the board game Chess. With a single gesture, a user can choose the color, type, and location of a piece on the board. We show how this generates a large password space at low gesture counts while still maintaining high memorability and usability.

Related Work

The original proposal for the *graphical password* is the patent filed by Blonder [1] in 1996. The graphical approach is based on the concept that the human brain is relatively weak at remembering sequences of numbers or letters, but excellent at processing visual data [1, 3]. This phenomenon is called the *picture superiority effect*, the notion that humans have a much greater capacity for processing and remembering visual data than numbers and letters [7, 5].

There are three types of graphical schemes, based on human memory *tasks* as outlined in [6]. In recognition based schemes, such as Deja Vu [2], the user is prompted to identify previously selected images. Recall based schemes, such as Draw-A-Secret [3], ask users to reproduce a secret drawing or gesture. Cued recall schemes, such as Passpoints [9], require users to perform actions on specific locations of an image or screen.

Mainstream mobile operating systems offer a few graphical schemes for authenication. The PIN based scheme, popularized by Apple, allows users to enter a 4-digit PIN on a number pad displaying the digits 0-9. 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. Windows devices use a cued recall scheme similar to Passpoints [9]. The scheme allows users to upload an image and create a password by drawing a series of three gestures (a gesture is considered a tap, line, or circle) on the image. There are also several schemes based on biometrics, such as the fingerprint scanner, but we will not address those schemes in this work.

According to our knowledge, this is the first attempt to formally define the concept of multi-dimension passwords and analyze their benefits in terms of memory interference, security, and usability. We filed a patent on MAPS [4].

Multi-Dimensional Password Scheme

The key idea of a MAPS is to form a password by fusing information from multiple dimensions. To better explain the design of a MAPS, we present an example MAPS based on the classic game of Chess.

Figures 1 and 2 shows two screen-shots of our implementation of the Chess-based MAPS (CMAPS) developed for Android systems. Users set a password by placing chess game pieces onto a board with 8×8 tiles. The resulting chess formation is a CMAPS password. An

[1] A larger gird is possible on some devices. We focus on the default size of the grid in this paper.

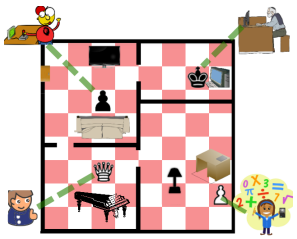

Figure 3: A sample graphical hint we generated to show to some of our participants.

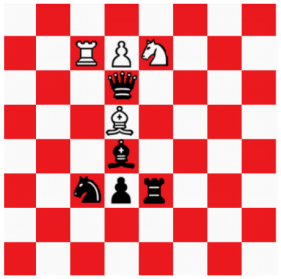

Figure 4: A CMAPS password generated by a user in our user study. The password is a cricket field, with different pieces denoting different players around the two wickets. The queen is the user's favorite player.

example password of CMAPS is shown in Figure 1. 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 2. The user can unlock the system by placing game pieces 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 allows a user to empty a tile.

A user can put a game piece onto the board with one line gesture connecting a selected game piece to a desired tile in the board, or two taps by touching the desired piece and then its desired location. No knowledge of chess is required to use CMAPS; the pieces can be placed anywhere on the board. We hypothesize that chess skills may help to memorize passwords because a user may use a formation with some game pieces related by attacking or defending.

As an example of MAPS, CMAPS fuses information from multiple dimensions. The dimensions used in CMAPS include the color of the game piece, the type of the game piece, and the row and column of the desired tile. CMAPS fuses the information from these dimensions with one gesture on a touch screen that puts a game piece onto the board.

Graphical Hints

We hypothesize that graphical hints can reduce the popularity of hotspots and increase memorability. These graphical hints are kept in the user's memory only. We show graphical hints as shown in Figure 3 to participants and ask them to generate their own. Figure 4 shows an example hint that one of the participants in our user study generated.

Usability Analysis

We can evaluate the usability of mobile schemes with two metrics: number of gestures required to finish one authentication and time needed to finish authentication. CMAPS users can place a game piece onto the board by a drawing a line between a selected game piece and a tile on the board. A CMAPS password having l game pieces can require l gestures to input. Since each gesture allows the user to choose color, piece type, and location, the password space is $2^l 6^l \binom{64}{l}$.

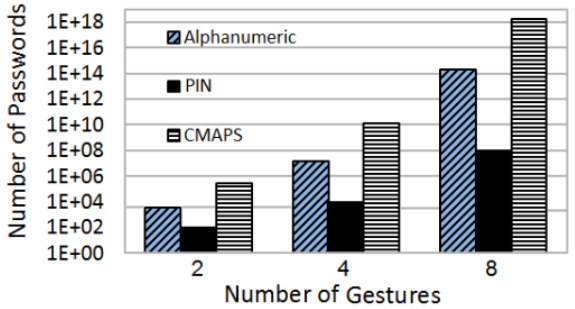

Figure 5: Number of Passwords supported by 2, 4, and 8 gestures

Figure 5 shows the number of passwords supported at low gesture counts using CMAPS, 4-digit PINs, and case-insensitive alphanumeric passwords. A password with 6 CMAPS gestures is stronger than an 8 character alphanumeric password used for secure applications like banking. We will discuss timing data collected from our user study in the next section.

User Study

We conducted a user study with 54 participants, 28 male and 26 female. Participants were asked to generate CMAPS passwords using 2, 8, or "8 or more" pieces. One

group was also asked to generate "8 or more" piece passwords with graphical hints. We call these groups 2g, 8g, 8+g, and 8+gh respectively.

Table 1: Recall Rates of CMAPS Passwords.

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

Table 1 shows the recall rates of CMAPS passwords in the four categories after one week. Our application also studied timing data during the experiment. Although they were not instructed to move quickly, participants required an average of 10, 16, 16, and 20 seconds to authenticate themselves in the 2g, 8g, 8+g, and 8+gh conditions respectively.

Discussion and Future Work

We plan to expand on the idea of MAPS by adding other games, e.g. Monopoly or Checkers. By giving users the ability to use different games, we hope to reduce memory interference between different MAPS passwords.

Acknowledgement

This work was supported in part by the US National Science Foundation under Grants CNS-1338105 and CNS-1343141.

References

[1] Blonder, G. Graphical password, sep 1996. Patent 5,559,961.

[2] Dhamija, R., and Perrig, A. Deja vu: A user study using images for authentication. In *Proceedings of the 9th Conference on USENIX Security Symposium - Volume 9*, SSYM'00, USENIX Association (Berkeley, CA, USA, 2000), 4–4.

[3] Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., and Rubin, A. D. The design and analysis of graphical passwords. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, SSYM'99, USENIX Association (Berkeley, CA, USA, 1999), 1–1.

[4] Manning, P., McLennan, C. T., and Zhu, Y. Authentication method for a computing device using interactive game board and game piece images, 2013. Patent 61782062.

[5] Nickerson, R. *Short-term Memory for Complex Meaningful Visual Configurations: a Demonstration of Capacity*. Defense Technical Information Center, 1964.

[6] Raaijmakers, J. G., and Shiffrin, R. M. Models for recall and recognition. *Annual review of psychology 43* (1992), 205–234.

[7] Shepard, R. Recognition memory for words, sentences, and pictures. *Journal of Verbal Learning and Verbal Behavior 6*, 1 (1967), 156 – 163.

[8] Stobert, E., and Biddle, R. Memory retrieval and graphical passwords. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, ACM (New York, NY, USA, 2013), 15:1–15:14.

[9] Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., and Memon, N. Passpoints: Design and longitudinal evaluation of a graphical password system. *Int. J. Hum.-Comput. Stud. 63*, 1-2 (July 2005), 102–127.