PassGame: A Shoulder-Surfing Resistant Mobile Authentication Scheme

Jonathan Gurary*, Ye Zhu*, Nahed Alnahash†, and Huirong Fu†
*Department of Electrical and Computer Engineering, Cleveland State University, Cleveland, Ohio
Emails: j.gurary@vikes.csuohio.edu, y.zhu61@csuohio.edu
†Department of Computer Science, Oakland University, Oakland, Michigan
Emails: nalnahas@oakland.edu, fu@oakland.edu

***Abstract*—Ubiquitous computing enabled by mobile devices, such as smartphones and tablets, causes more exposure of device users to shoulder-surfing attacks in crowded places, such as a subway train. In this paper, we propose *PassGame*, a shoulder-surfing resistant mobile authentication scheme based on board games. The design of PassGame is based on the popular game of chess. PassGame challenges a user with a random formation of chess pieces on a game board. A successful authentication requires a user to respond to the challenge so that a set of predefined rules are satisfied after adjustments made by the user. PassGame can be finished by a user without any chess knowledge. We implement PassGame on the Android operating system. Our user studies with the Android implementation show that PassGame passwords with more password strength than current mobile authentication schemes can achieve 100% recall rates when recalled one week after password setup.**

Keywords–Shoulder Surfing; Challenge Response; Gamification; Mobile Authentication; Graphical Passwords

I. INTRODUCTION

Mobile devices, such as smartphones and tablets, are becoming increasingly popular because of their nearly ubiquitous Internet access through various communication capabilities such as WIFI, 3G, or 4G networks and their numerous applications and games. While users are enjoying the benefits of ubiquitous computing enabled by mobile devices, they are also becoming more vulnerable to shoulder-surfing attacks. Consider a user on a crowded subway train. The user may want to check emails as there are a few stops before a destination. But, to check emails through a smartphone, the user has to unlock the screen with possibly several pairs of eyes watching the whole authentication process from behind. Since current authentication schemes on mobile devices are not designed to resist shoulder-surfing attacks [1], users of mobile devices are in danger of password theft and its consequences such as data breach from their mobile devices. Research suggests that mobile phone users unlock their devices an average of 48 times per day (about 3 unlocks per hour), and users perceive shoulder-surfing to be possible in 17% of these instances [2].

Designing an authentication scheme for mobile devices is a challenging task because the scheme should be both *secure* and *usable*. For mobile devices, a secure authentication scheme should be shoulder-surfing resistant for ubiquitous computing and the scheme should have a large password space, i.e., a large number of possible passwords. Usability of an authentication scheme is of the same importance for mobile devices: (1) The scheme should be easy to use. (2) Passwords generated by the scheme should be easy to remember.

In this paper, we propose *PassGame*, a shoulder-surfing resistant mobile authentication scheme based on board games. PassGame is essentially a challenge-response authentication scheme. In our current design, PassGame is based on the popular game of chess. An authentication starts with a random chess board, i.e., a chess board with randomly selected game pieces on randomly selected tiles of a game board. The random chess board serves as a challenge to the user. To finish the authentication successfully, the user responds to a challenge by making adjustments to the random game board so that a set of predefined rules are satisfied. The adjustments can be moving game pieces, adding new game pieces, and removing existing game pieces. PassGame supports both rules without any requirements on chess knowledge and rules requiring only basic chess knowledge.

In general, shoulder-surfing resistant schemes incur relatively higher usability costs such as longer password entry time. PassGame is not designed to replace existing mobile authentication schemes, such as Google's pattern unlock and the four-digit PIN widely used on smartphones. Instead PassGame can be a supplemental scheme for use in crowded places or places with camera surveillance. PassGame can also be a choice for high security authentications on smartphone operating systems supporting different security levels in authentication such as Android.

The rest of the paper is organized as follows: We review related work on graphical passwords and shoulder-surfing resistant authentication schemes in Section II. Then, we present the design details of PassGame in Section III. We present our user studies on the usability and memorability of PassGame in Section IV. We conclude the paper in Section V.

II. RELATED WORK

A number of research efforts have been aimed to add shoulder-surfing resistance into existing schemes. Roth *et al.* [3] proposed to add the resistance to the classic 4-digit PIN by splitting the PIN entry pad into two sets (black and white buttons) and asking users to choose which set their digit is in. The process is repeated several times to confirm the choice of a digit and repeats again until all the digits are chosen. Since then many schemes to add shoulder-surfing resistance to the 4-digit PIN have been proposed, including SwiPIN [4], ColorPIN [5], and The Phone Lock [6]. While

 ISBN: 978-1-61208-538-8

these schemes can improve shoulder-surfing resistance of PIN-based schemes, these schemes still suffer from inherently weak security strength in PINs and these schemes can be easily compromised by brute force attacks.

Zakaria *et al.* [7] proposed to improve the shoulder-surfing resistance of Draw a Secret [8] by erasing strokes as they are drawn. Their user study shows the improvement can reduce the rate of medium-strength passwords captured by an attacker after a single observation from 80% to roughly 40%. Lin *et al.* [9] proposed to add a grid to Draw A Secret. In addition to matching the Draw a Secret gesture, users in this scheme must also match the direction (e.g., up, down) in which some strokes of their gesture pass through the added grid lines.

Convex Hull Click (CHC) [10] is a graphical password scheme designed to counter shoulder-surfing attacks. CHC asks users to choose icons to represent their passwords. Rather than clicking the icons, users are required to click somewhere inside the triangular area bounded by their chosen icons. CHC suffers from long authentication times because multiple click sessions are required and it takes time for the user to find their icons. The CDS scheme [11], a combination of Draw a Secret [8] and Story [12], arranges a series of images randomly into a grid and asks users to draw a line through the images they choose to represent their passwords.

A number of shoulder-surfing resistant schemes require extra hardware [6], [13], [14], [15]. These schemes may not be suitable for mobile authentication because of hardware and software requirements and smaller screens on mobile devices.

PassGame can be considered a multi-dimensional password, as proposed in [16]. PassGame uses many dimensions such as rule, color, piece type, and number of attacking pieces.

III. The PassGame Design

In this section, we present an overview of PassGame and describe the design details of PassGame.

A. Overview

The current design of PassGame is based on the popular game chess. PassGame is essentially a challenge-response authentication scheme. In PassGame, a mobile device challenges a user with a randomly generated chess board, i.e., a chess board with randomly selected game pieces placed on randomly selected tiles. The user responds to the challenge by making adjustments on the chess game board including adding new games pieces, removing existing game pieces, and moving existing game pieces. A correct response will be an adjusted game board satisfying some predefined rules. For example, one rule of PassGame is to move game pieces by n_{tile} tiles in total. Any move of a game piece including illegal moves in the chess game is allowed. Moving a game piece to the right or the left by one tile adds or decreases one tile from the total respectively. Similarly, moving a game piece up or down by one row adds or decreases eight tiles from the total, respectively, as one row in the chess board has 8 tiles. A user can also add or decrease the number of tiles moved by adding a new game piece to the board or removing a game piece from the board respectively. As long as the sum of total tiles moved is equal to n_{tile}, the predefined number of tiles in total, the rule is satisfied and the user will be authenticated if no other rules are in use. Otherwise, the authentication is unsuccessful.

PassGame supports both rules without any requirements on chess knowledge and rules requiring basic chess knowledge. The design is to make sure every user, including those who have no knowledge of the chess game, can use the authentication scheme. The other rules require only basic chess knowledge of how game pieces attack. We include these rules requiring basic knowledge of chess to take advantage of the popularity of chess because we hypothesize that chess knowledge or previous experiences in chess games may improve memorability of PassGame passwords.

A PassGame password can be formed with multiple rules. In general, using more rules to form a PassGame password can make the PassGame password more complex, and in turn more resistant to brute force attacks and shoulder-surfing attacks.

As long as the rules of a password are satisfied, PassGame allows users to make unrelated adjustments to the board. In other words, a user can add, remove, and move game pieces that are not involved in any rules used to form a password. These unrelated adjustments to a game board allow a user to further mitigate shoulder-surfing attacks as a shoulder-surfer can not tell which game pieces are involved in the rules used to form the PassGame password.

To make PassGame more usable, the design does not enforce laws of chess. Any piece of either color can be positioned on any tile of the chess board, and multiple pieces of the same type are permitted (e.g., three kings).

In the rest of this section, we describe the generation of a random game board and then the details of each rule possibly used in a PassGame password.

B. Random Board Generation

Since PassGame authentication starts with a challenge of a random board, the generation of the random board is important for both the security and usability of PassGame. On each tile, there are 13 possibilities: the tile is empty, or it is occupied by a king, queen, bishop, knight, rook, or pawn in either of the two colors.

PassGame randomly selects one from the 13 possibilities for each tile. Pieces appear with the same frequency as they typically appear in chess middlegame, though it is also possible to get boards which are almost completely empty or full. The design is to ensure most boards have enough pieces so that there are many ways to satisfy the rules of a password.

We allow a user to request a new random board and get authenticated with the new random board. A user may request a random board for several possible reasons: (1) The user's password cannot be completed on the given random board (e.g., remove 3 black pieces from the board on a board with less than 3 pieces), (2) The user wants a board where the password can be input more easily, (3) The user wants to find a game board where shoulder-surfing is less likely, or (4) The user has modified the random board unsuccessfully and does not remember what it initially looked like. A random board often partially or completely satisfies some of a user's rules without any modifications. Thus, a shoulder-surfer may not

 ISBN: 978-1-61208-538-8

necessarily see the user inputting all the rules that comprise their password, forcing them to guess remaining rules from the contents of the random board.

C. PassGame Rules

In our current design, a PassGame password can be formed with 12 rules. We present the details of the rules below.

The first 6 rules do not require any chess knowledge. So, any user should be able to use these rules.

Rule R1: Number of Tiles Moved in Total: The parameter of this rule is the number of tiles moved. To satisfy this rule, a user must make adjustments to a game board so that the number of tiles moved in total should be equal to a predefined number n_{tile}. The board can be considered as a numbered grid from 1 to 64, where the bottom left corner is 1, and the top right is 64. Moving a game piece to the right or to the left by one tile adds or decreases the number of tiles moved in total by one respectively. Similarly, moving a game piece up or down by one row adds or decreases the number of tiles moved in total by 8 respectively. Adding a game piece to a tile adds to the number of tiles moved in total by the number associated with that tile. On the contrary, removing a game piece from a tile decreases the number of tiles moved in total by the number associated with that tile.

For example, if a user sets $n_{tile} = 8$ in the password setup phase, the user can satisfy this rule by adding a piece to tile 8 if the tile is not occupied, or by moving a piece on tile 12 to tile 20 if the destination tile is not occupied. To mitigate shoulder-surfing attacks, a user can also combine multiple adjustments together to achieve the number of tiles in total. For example, if $n_{tile} = 8$, a user can move one piece forward by 20 tiles, move another piece backwards by 10 tiles, add a piece to tile 28, and remove a piece from tile 30 to make the number of total tiles moved be 8. In theory, the range of n_{tile} is $[-2080, 2080]$ as $\sum_{i=1}^{64} i = 2080$.

Rule R2: Number of Pieces in a Row: The parameters of this rule are color, row index, and number of pieces of the selected color that must exist in the selected row. To satisfy this rule, a user must adjust a game board so that the selected row has the chosen number of pieces in it of the chosen color. This can be done adding pieces or removing pieces from the row, as a randomly generated row may have more pieces than are needed. The number of possible combinations of the parameters is $3 \times 8 \times 8 = 192$ as (1) color can be black, white, or both, and (2) a chess board has 8 rows and columns.

Rule R3: Number of Pieces in a Column: This rule is similar to Rule R2 and the only difference is that R3 is defined on a column. So the number of possible combinations of the parameters is also 192.

Rule R4: Number of Pieces on a Board: This rule is similar as Rule R2 and the only difference is that R4 is defined on a game board. The parameters of this rule are color and number of pieces on the board, so the number of possible combinations of the parameters is $3 \times 64 = 192$ as (1) color can be black, white, or both and (2) a board can hold up to 64 game pieces.

Rule R5: More or Less Pieces: The parameters of this rule are color and the number of pieces added or removed from a board. To satisfy this rule, a user must add or remove the specified number of pieces in the chosen color. To further mitigate shoulder-surfing attacks, a user may want to add and remove pieces several times. As long as the final number of pieces added or removed from a board totals the specified number, the rule is satisfied. The number of possible combinations of the parameters is $3 \times 64 \times 2 = 384$ because (1) color can be black, white, or both, (2) at most 64 pieces can be added or removed from the board.

Rule R6: Specific Tile: The parameters of this rule are piece type, color, row index, and column index. The rule is satisfied when the specified piece of the chosen color is at the chosen row and column location. The number of possible combinations of the parameters is $6 \times 3 \times 8 \times 8 = 1152$ as (1) the piece type can be king, queen, bishop, knight, rook, or pawn, (2) the color can be black, white, or both colors, and (3) the board has 8 rows and 8 columns.

The next 6 rules require only basic knowledge of attacks in chess. To add more attacks, a user can add game pieces under attack, attack existing pieces, or both. Attacks can also be added by removing pieces blocking attack paths of other game pieces. Similarly, attacks can be reduced by adding blocking pieces, removing attacking pieces, or removing the pieces under attack.

Rule R7: Number of Attacks on a Piece: The parameters of this rule are piece type, piece color, and number of attacks. This rule is satisfied when a game piece of the type and color selected is attacked by the chosen number of attackers. One example is that a bishop of either color is under attack by five pieces. If there is no such piece on a random board, a user can add it to the board. If there are multiple such pieces a board, then only one of them is required to be under attack by the specified number of pieces. The number of possible combinations of the parameters is approximately $6 \times 3 \times 16 = 288$ as (1) the piece type can be king, queen, bishop, knight, rook, or pawn, (2) the color can be black, white, or both colors, and (3) the maximum number of attacks to one tile is 16 (4 diagonal attacks, 2 horizontal attacks, 2 vertical attacks, and 8 attacks by knights). Note that not every tile can have 16 attackers (e.g corner tiles can have a maximum of 5 attackers), so it may be necessary to move a piece or place a new one in order to satisfy larger numbers of attacks.

Rule R8: Number of Attacks by Pieces: The parameters of this rule are piece type, piece color, and number of attacks. The rule is satisfied when a game piece of the selected type and color is attacking the chosen number of game pieces. For a king, a queen, or a knight, there are $3 \times 8 = 24$ combinations because (1) color can be black, white, or both and (2) a king, a queen, or a knight can attack a maximum of 8 pieces. For a bishop or a rook, there are $3 \times 4 = 12$ combinations because a bishop or a rook can attack 4 pieces at most. For a pawn, there are only $3 \times 2 = 6$ combinations because a pawn can only attack two pieces at most. So the total number of possible combinations is $3 \times 24 + 2 \times 12 + 6 = 102$.

Rule R9: Number of Pieces under Attack: The parameters of this are piece color and number of pieces under attack. The rule is satisfied when the selected number of game pieces of the chosen color are under attack. Since (1) the maximum

 ISBN: 978-1-61208-538-8

Figure 1. A screenshot of the PassGame application.

number of attacks is 64 when a board is filled and every game piece is under attack, and (2) color can be black, white, or both, the number of possible combinations is $3 \times 64 = 192$.

Rule R10: More or Less Attacks on A Piece: The parameters of this rule are piece type, piece color, and number of attacks to add or remove. The rule is satisfied when the selected number of attacks are added or removed from a game piece of the chosen type and color. If there is no such piece on the board, a user can add it. As described in Rule R7, the maximum number of attacks on one tile is 16. Since (1) color can be black, white, or both and (2) the piece type can be king, queen, bishop, knight, rook, or pawn, the number of possible combinations is $3 \times 6 \times 32 = 576$.

Rule R11: More or Less Attacks by A Piece: The parameters of this rule are piece type, piece color, and number of attacks to add. The rule is satisfied when the selected number of attacks are added or removed from a piece of the chosen color and type. A king, queen, or knight can attack 8 pieces at most. In other words, a user can select any of the 16 possible values between -8 and 8. The number of possible combinations for a king, queen, or knight is $3 \times 16 = 48$ since color can be black, white, or both. A bishop or rook can attack a maximum of 4 pieces, so the number of possible combinations for a bishop or a rook is $3 \times 8 = 24$. A pawn can attack up to 2 pieces, so the number of possible combinations for a pawn is $3 \times 4 = 12$. The total number of combinations is 204.

Rule R12: More or Less Pieces under Attack: The rule parameters are piece color and number of attacks to add or remove. This rule is satisfied when a user adds or removes the selected number of attacks to game pieces in the chosen color. A user can add or remove up to 64 attacks. The number of possible combinations of the parameters is $3 \times 128 = 384$ since color can be black, white, or both.

IV. User Study

We implemented PassGame on the Android operating system. A screenshot of the implementation is shown in Figure 1. To evaluate PassGame, we conducted user studies with participants recruited from two university communities. We used a Samsumg Galaxy Tab 3 with a 7 inch 1024×600 display and the Samsung S4 with a 5 inch 1920×1080 display.

Procedure: On the first day, participants come to our laboratory to fill out demographic information, learn the ChessPass scheme, and set a password. Before they leave the laboratory, participants must successfully authenticate themselves twice on two different random boards.

Similar to previous studies [17], we asked participants to use PassGame during the one-week-long user study to simulate regular use of the authentication scheme. We sent an email to participants 3-4 days after the first session then again 5-6 days after the first session. The email contains a link to an emulated version of the PassGame application hosted on sites.google.com/. The emulated version uses the same code and behaves in the same way as the version that participants used during the first session. We use an emulated version rather than asking participants to return to the laboratory to use the device because it is more convenient for participants and this portion of the experiment is designed solely to simulate regular use of the scheme. Use of the emulator is encouraged but not mandatory because (1) email responses are not reliable because of various reasons such as junk mail filtering, (2) we want to investigate the effect of regular use on the memorability of PassGame. Each participant had at most two successful authentications on the emulator and the attempts on the emulator happened within 36 hours from the sending time of the reminder emails.

One week after the first session, participants are invited back to the controlled laboratory environment for the second session. Participants are given the mobile device that they used during the first session and are asked to recall their passwords. At the end of the second session, participants are asked to fill out a survey rating the usability of PassGame and their favorite mobile authentication scheme.

Conditions: To evaluate the usability of PassGame with different security strength, participants were randomly grouped into one of three categories: (1) 1R: Participants in this condition were asked to make a password using a single rule. (2) 2R: Participants in this condition were asked to make a password with two rules. (3) 4R: Participants in this condition were asked to make a password with four rules. Participants are not allowed to form a password with Rule R6 only as the resulting password may not be shoulder-surfing resistant if no unrelated adjustments are included into the password. So, participants in 1R category are not allowed to use Rule R6.

Participants: We recruited participants for the user studies by distributing fliers and leaflet style advertisements. A $10 cash incentive was offered for completing both sessions of the user study. Thirty seven participants were recruited for the user studies and 36 successfully finished both sessions. Of those who finished, 23 participants were male and 13 were female. 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 an average of 4.28, with 32 rating their skill at 4 or higher.

Statistical Testing: We use a significance level of .05 for our hypothesis testing in this paper. For omnibus comparisons on categorical and quantitative data, we use Chi-squared and Kruskal-Wallis respectively. If the omnibus test is significant, we perform pairwise tests with Chi-squared for categorical data and Mann-Whitney for quantitative data.

 ISBN: 978-1-61208-538-8

TABLE I. PASSGAME RECALL RATES BY CONDITION

Conditions	Participants	Recall	Recall Rate
$1R$	12	12	100%
$2R$	14	14	100%
$4R$	10	7	70%

A. Memorability Results

As a PassGame password formed with more rules requires more rule selections and rule parameters to be memorized, we hypothesize that the recall rate of PassGame passwords decreases when the number of rules used to form PassGame passwords increases.

The recall results of the user study are shown in Table I. The results show that none of our participants had any trouble in remembering 1R or 2R passwords. The recall rate of 4R passwords is 30% lower than the rates of 1R and 2R passwords, but most participants were still able to remember their 4R passwords as well. We perform an omnibus chi-squared test on the three conditions and find a significant difference between the memorability of the conditions ($\chi^2 = 8.51$, $p = .014$). The hypothesis is supported by the data of PassGame passwords formed by 4 or less rules. We believe that the statistical difference will become more significant when the number of rules used to form a PassGame password is larger. We restrict our user study on PassGame passwords formed with no more than 4 rules because (1) a two-rule password already has more password strength than passwords of existing mobile authentication schemes, such as 4-digit PIN, and (2) PassGame passwords formed with more than 4 rules are less usable.

We examine the effect of the reminder emails on memorability. We hypothesize that using the emulator during the week will make participants more likely to remember their passwords at the end of the week. Five participants used the emulator only after receiving the first reminder email, 2 used the emulator only after receiving the second reminder email, 24 used the emulator both times, and 5 did not use the emulator at all. The omnibus chi-squared test reveals no significance ($\chi^2 = 1.64$, $p = .651$). All three participants who forget their passwords used the emulator both times, and were unable to finish authentication successfully either time. The results suggest that PassGame passwords are memorable after one week even with no reminders.

We hypothesize that chess knowledge has an impact on memorability. Thirty-one participants indicated that they knew how to play chess, while 5 indicated they did not know how to play chess. Among the 3 participants that forgot their passwords, 2 knew how to play chess and 1 did not. Our omnibus chi-squared test reveals that there is no significant difference ($\chi^2 = 1.04$, $p = .309$). The results are not compliant with our expectation. But, the results also indicate that the scheme is memorable even by persons who have no knowledge of chess.

B. Password Entry Time

Our implementation records the time users spend attempting to enter their passwords. In this section, we analyze the timing data from the final session of the user study.

On average, users in the 1R, 2R, and 4R conditions required 33, 110, and 143 seconds respectively to authenticate themselves from the moment they started the application. A Kruskal Wallis test between the three conditions finds no significant difference (H=4.996, p=.082). However, these timings values include time spent thinking, requesting new boards, and making incorrect attempts. On average, users required 1.6, 1.9, and 2.1 new randomly generated boards for the 1R, 2R, and 4R conditions respectively before successfully entering their passwords. Additionally, users required an average of 1.22, 2.07, and 2.63 authentication attempts before a success for 1R, 2R, and 4R respectively. The first correct attempt in the 1R, 2R, and 4R conditions required on average 23, 44, and 49 seconds respectively. The best 4 users in 1R required less than 7s to authenticate. We perform a Kruskal Wallis test on the timings for the first correct attempt and find that there is not a significant difference in the timings (H=3.741, p=.154).

TABLE II. USABILITY SURVEY RATINGS

Scheme	Ratings	Conve.	Speed
PassGame-1R	4	4.5	4.25
PassGame-2R	7	4.29	3.29
PassGame-4R	7	3.75	2.57
PassGame-all	7	4.06	3.22
4-digit PIN	10	5	5

We believe that these statistics will improve as users gain experience with the scheme, in particular we believe users will require fewer attempts as they get used to the scheme. Password entry times for a single correct attempt are already very similar between the conditions. The entry times for correct attempts is in line with other schemes such as Deja Vu (32s) [18], Delayed Oracle Choice PIN entry (25s) [3], or CDS (20s) [11] and superior to other shoulder-surfing resistant schemes like Convex Hull Click (72s) [10].

SwiPin [4], ColorPIN [5], The Phone Lock [6], and other schemes that improve on PIN or pattern unlock offer short login times, but at the cost of weak password strength and limited shoulder-surfing resistance. PassGame can be used as a supplementary high-security scheme in environments where the user is afraid of shoulder-surfing. The user may be willing to trade off entry time in exchange for security in these situations.

C. User Perception

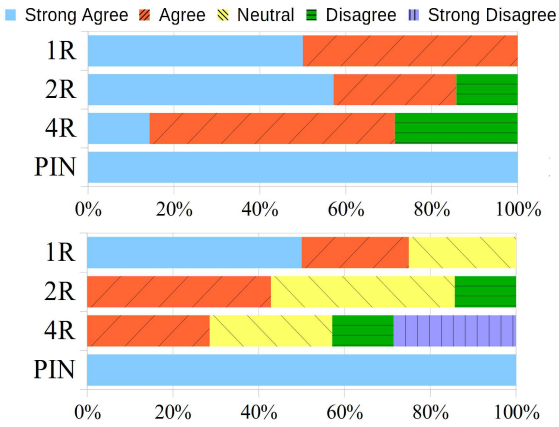

Figure 2. Usability Survey for Convenience (top), Speed (bottom).

At the end of the user study we asked participants to fill out

a survey regarding the usability of PassGame and their current favorite authentication scheme. Participants were asked to rate the following statements (once for PassGame, and once for their favorite scheme) on a scale from "Strongly Disagree" (1) to "Strongly Agree" (5): (a) It is convenient to enter a password using this scheme. (b) The speed of entering a password with this scheme is fast. Additionally, we provide participants with the following definitions as a guideline: (a) Convenience: The scheme does not restrict you or take too much attention, (b) Speed: You can finish the scheme quickly. It usually does not need too many tries. For their favorite scheme, 10 participants chose 4-digit PIN, 2 participants chose Google's pattern unlock scheme, 3 chose fingerprint scanner. We sorted the usability results for PassGame based on which condition users were assigned to. The results of the usability survey are shown in Figure 2. The average usability rating is shown in Table II. For statistical analysis, we sort the usability ratings into the categories agree (4 or higher) or do not agree (3 or lower). We hypothesize that most users will think that PassGame is roughly as convenient as the 4-digit PIN or Google's pattern unlock scheme. We also hypothesize that the speed rating will decline as more rules are used. A chi-squared omnibus test on the three conditions of PassGame plus 4-digit PIN shows no significant difference in convenience ($\chi^2 = 4.11$, $p = .25$), however there is a significant different in speed ($\chi^2 = 11.04$, $p = .01$). Pairwise testing reveals the results are significant between 2R and 4-digit PIN ($\chi^2 = 7.47$, $p < .01$) and between 4R and 4-digit PIN ($\chi^2 = 10.12$, $p < .01$). At 2 rules and up, users perceive PassGame to be a slower scheme than the 4-digit PIN. We believe the difference is mainly caused by the shoulder-surfing resistance. A user usually repeats a 4-digit PIN without any thinking. But a user of shoulder-surfing resistant schemes needs to think out a valid response to a random challenge. Another possible reason is the difference in the familiarity to the scheme as the participants may be using the 4-digit PIN scheme everyday on their mobile devices and they only used PassGame for a few times.

Due to the space limit, we leave the analysis on shoulder-surfing resistance of PassGame with information theory, password space analysis, and extension of the authentication scheme in the technical report [19].

V. Conclusion

We designed PassGame to mitigate shoulder-surfing attacks on mobile authentication. We implemented PassGame on the Android operating system and conducted a user study. Our user study shows that PassGame passwords, which greatly exceed the password strength of current mobile authentication schemes, can still achieve 100% recall rates when recalled one week after password setup. In our future work, we plan to test PassGame against more sophisticated shoulder-surfing attacks, for example a machine-assisted brute force based on camera recorded password entries, and to test the viability of other games such as Checkers or Backgammon.

Acknowledgment

This work was supported in part by the National Science Foundation under Grants CNS-1460897, CNS-1338105, CNS-1343141, and DGE-1623713. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding agencies.

References

[1] X. Suo, Y. Zhu, and G. Owen, "Graphical passwords: a survey," in *Computer Security Applications Conference, 21st Annual*, Dec 2005, pp. pp.462–472.

[2] M. Harbach, E. von Zezschwitz, A. Fichtner, A. D. Luca, and M. Smith, "It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception," in *Symp. On Usable Privacy and Security*. Menlo Park, CA: USENIX Association, 2014, pp. 213–230.

[3] V. Roth, K. Richter, and R. Freidinger, "A pin-entry method resilient against shoulder surfing," in *Proceedings of the 11th ACM Conference on Computer and Communications Security*, 2004, pp. 236–245.

[4] E. von Zezschwitz, A. De Luca, B. Brunkow, and H. Hussmann, "Swipin: Fast and secure pin-entry on smartphones," in *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, vol. 15, 2015, pp. 1403–1406.

[5] A. De Luca, K. Hertzschuch, and H. Hussmann, "Colorpin: securing pin entry through indirect input," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2010, pp. 1103–1106.

[6] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, "The phone lock: audio and haptic shoulder-surfing resistant pin entry methods for mobile devices," in *Proc. of the Fifth International Conf. on Tangible, Embedded, and Embodied Interaction*. ACM, 2011, pp. 197–200.

[7] N. H. Zakaria, D. Griffiths, S. Brostoff, and J. Yan, "Shoulder surfing defence for recall-based graphical passwords," in *Proceedings of the 7th Symposium on Usable Privacy and Security (SOUPS)*, 2011, pp. 1–12.

[8] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in *Proc. of the 8th Conf. on USENIX Security Symp.*, Berkeley, CA, USA, 1999, pp. 1–14.

[9] D. Lin, P. Dunphy, P. Olivier, and J. Yan, "Graphical passwords & qualitative spatial relations," in *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS)*, 2007, pp. 161–162.

[10] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *Proceedings of the Working Conference on Advanced Visual Interfaces (AVI)*, 2006, pp. 177–184.

[11] H. Gao, Z. Ren, X. Chang, X. Liu, and U. Aickelin, "A new graphical password scheme resistant to shoulder-surfing," in *International Conference on Cyberworlds (CW)*. IEEE, 2010, pp. 194–199.

[12] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in *Proceedings of the 13th Conference on USENIX Security Symposium*, Berkeley, CA, USA, 2004, pp. 1–11.

[13] D. Luca *et al.*, "Back-of-device authentication on smartphones," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, 2013, pp. 2389–2398.

[14] C. Winkler *et al.*, "Glass unlock: Enhancing security of smartphone unlocking through leveraging a private near-eye display," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, CHI*, vol. 15, 2015, pp. 1407–1410.

[15] A. De Luca, E. Von Zezschwitz, and H. Hußmann, "Vibrapass: secure authentication based on shared lies," in *Proc. of the SIGCHI conf. on human factors in computing systems*. ACM, 2009, pp. 913–916.

[16] J. Gurary, Y. Zhu, G. Corser, J. Oluoch, N. Alnahash, and H. Fu, "Maps: A multi-dimensional password scheme for mobile authentication," in *Proceedings of the 2015 International Conference on Interactive Tabletops & Surfaces*. ACM, 2015, pp. 409–412.

[17] N. Wright, A. S. Patrick, and R. Biddle, "Do you see your password?: Applying recognition to textual passwords," in *Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS)*, 2012, pp. 1–14.

[18] R. Dhamija and A. Perrig, "Deja vu: A user study using images for authentication," in *Proceedings of the 9th Conference on USENIX Security Symposium*, Berkeley, CA, USA, 2000, pp. 1–4.

[19] J. Gurary, Y. Zhu, N. Alnahash, and H. Fu, "Passgame: A shoulder-surfing resistant mobile authentication scheme, technical report 20161101a," Oct 2016, retrieved: Jan 2017. [Online]. Available: http://academic.csuohio.edu/zhu_y/techreport/20161101a.pdf

 ISBN: 978-1-61208-538-8