An Ancient Indian Board Game as a Tool for Authentication

Sreelatha Malempati[1] and Shashi Mogalla[2]

[1] Department of Computer Science and Engineering
RVR & JC College of Engineering, Guntur, A.P.
e-mail: lathamoturi@rediffmail.com

[2] Department of Computer Science and System Engineering
Andhra University College of Engineering, Visakhapatnam, A.P
e-mail: smogalla2000@yahoo.com

Abstract: User authentication is the first phase of information security. Users should remember their passwords and recall them for authentication. Text based passwords is the traditional method for authentication. Short and simple passwords are memorable and usable but not secure. Random and lengthy passwords are secure but not memorable and usable. Graphical password schemes are introduced as alternatives to text based schemes. Few grid based authentication techniques are also proposed. The purpose of this paper is to introduce a tool to enhance the memorability and security of passwords which also provides usability. The most popular ancient Indian board game "**Snakes and Ladders**" is used as a tool for authentication.

Keywords: Intrusion prevention, Graphical passwords, Snakes & Ladders game, memorability of passwords .

1. INTRODUCTION

Authentication refers to the process of confirming or denying an individual's claimed identity. User authentication is the first phase of information security. Users should remember their passwords and recall them for authentication. Current authentication methods can be divided into three main areas: Knowledge based authentication, token based authentication and biometric based authentication. Knowledge based authentication techniques are most widely used and include text-based and picture-based passwords. Credit card is an example for token based authentication technique. Fingerprints, iris scan, or facial recognition are examples of biometric based authentication. The major drawbacks of token based and biometric based authentication methods are expensive and requires special devices. Textual passwords are first choice for authentication by humans. Due to the limitation of human memory, users generally choose the passwords which are easy to remember. The strength of the password depends on size of the memorable password space rather than full password space. Short and simple passwords are memorable and usable but not secure. Random and lengthy passwords are secure but not memorable and usable. Graphical password schemes are introduced as alternatives to text based schemes.

Strong password policies[1] may be adopted by the organizations for secure passwords. Those policies typically increase the burden on the users' ability to remember the passwords [2]. For an effective authentication scheme, passwords must be memorable, usable and secure. According to DTI survey[3], an average user has to remember three different job-related user IDs and passwords. Some employees need to remember more than 10 passwords. In addition, each user has to remember many personal passwords for banking, e-commerce, email accounts

and social networking accounts. As the number of passwords to remember increase, it is difficult for the human to recall the passwords.

Graphical authentication schemes are introduced as alternatives to text-based passwords. Cognitive studies have shown that people are much better at recognizing previously seen images than at recalling text precisely. Graphical password schemes can be grouped into three classes based on the type of cognitive activity required to remember the password: recognition, pure recall, and cued recall [4,5]. Recognition is the easiest one for human memory whereas pure recall is most difficult since the information must be accessed from memory without cues. Traditional password schemes are examples for pure recall. Cued recall provides cues to users that are associated with the password which helps to recall their passwords [5].

The short and simple passwords are easy to remember. But it is easy to break the password. Random and lengthy passwords are more secure but difficult to remember. This paper proposes to use a tool to select lengthy and memorable passwords. Psychology studies have revealed that the human brain is better at recognizing and recalling images than text[6]. A cued recall scheme is used to increase the memorability of passwords. As a well known tool is being used for password memorability and security, it also provides usability of passwords .

Snakes and ladders is an ancient Indian board game that is now a worldwide classic. It is played between 2 or more players on a playing board with numbered grid squares. On certain squares on the grid are drawn a number of "ladders" connecting two squares together, and a number of "snakes" also connecting squares together. The size of the grid (most commonly 8×8, 10×10 or 12×12) varies from board to board. Each player starts with a token in the starting square and takes turns to roll a single die to move the token by the number of squares indicated by the die roll, following a fixed route marked on the gameboard from the bottom to the top of the playing area, passing once through every square. If, on completion of this move, they land on the lower-numbered end of the squares with a "ladder", they can move their token up to the higher-numbered square. If they land on the higher-numbered square of a pair with a "snake" they must move their token down to the lower-numbered square. The winner is the player whose token first reaches the last square of the track. This game is used for authentication to improve the memorability, usability and security of passwords. This tool is especially useful for rural people to remember lengthy passwords.

This paper is organized as follows: Related work is presented in section 2; in section 3 the authentication scheme based on the tool is proposed; security analysis is done in section 4; user study is given in section 5 and conclusion is proposed in chapter 6.

2. RELATED WORK

Many graphical authentication schemes have been proposed. Blonder[7] suggested a technique, whereby a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of those locations. Dhamija and perrig [8] proposed a graphical authentication scheme in which the user selects certain number of images from a set of random pictures during registration. Later user has to identify the pre-selected images for authentication. The users are presented a set of pictures on the interface, some of them taken from their portfolio, and some images selected randomly. For successful authentication, users have to select 'their' pictures amongst the distractors. Weinshall and Kirkpatrick [9] proposed authentication schemes picture recognition, object recognition & pseudo word recognition and declared that pictures are most effective than the other two proposed schemes. More graphical password schemes have been summarized in a recent survey paper [10].

Few grid based schemes are proposed which uses recall method. Jermin et al [11] proposed a technique called "Draw A Secret" (DAS) where a user draws the password on a 2D grid. The coordinates of this drawing on the grid are stored in order. During authentication user must redraw the picture. The user is authenticated if the drawing touches the grid in the same order. The major drawback of DAS is that diagonal lines are difficult to draw and difficulties might arise when the user chooses a drawing that contains strokes that pass too close to a grid-line. Users have to draw their input sufficiently away from the grid lines and intersections in order to enter the password correctly. If a user draws a password close to the grid lines or intersections, the scheme may not distinguish which cell the user is choosing.

Wiedenbeck et al [12] proposed PassPoints in which passwords could be composed of several points on an image. They examined the usability of PassPoints in three separate in-lab user studies to compare text passwords to PassPoints and to verify the usability of PassPoints . Goldberg et al[13] conducted a small scale user study on a similar scheme Passdoodle. Thirteen participants took part in the study and each of them was asked to draw passdoodles using a pen and paper, rather than in a real system. Passdoodles were required to consist of at least two strokes and could be drawn in multiple colors. A doodle is considered as a full match if it is drawn in exactly the same order as when the user initially drew the passdoodle, and is considered as a visual match if it is not a full match due to stroke order, stroke direction, or number of strokes. They found that the order in which a password is drawn introduced much complexity to graphical passwords and suggested to neglect the order.

Chiasson et al[14] proposed a cued-recall graphical password technique. Users click on one point per image for a sequence of images. The next image displayed is based on the previous click point so users receive implicit feedback as to whether they are on the correct path when logging in. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. The visual cue does not explicitly reveal right or wrong but is evident using knowledge only the legitimate user should possess.

Luca et al [15] evaluated different authentication techniques for ATM usage. During the experimentations they found that many users tend to support their memory for their 4-digit-PINs by incorporating the layout of the digits on the number pad and the shape resulting from these spatial relations. Figure 1 shows an example: when entering the PIN 7197 a triangle is made on the number pad. This shape is used by many users to support their memory.

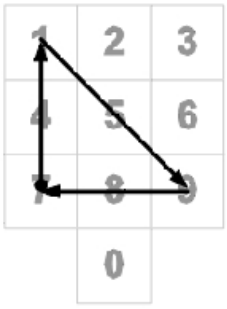

Figure 1: A shape used to remember the PIN 7-1-9-7

Luca et al[16] in the PassShapes concept, eliminate PINs as authentication tokens and used simple geometric shapes instead. These PassShapes are composed of strokes. There are eight different possible strokes defined which are shown in Figure 2. Several strokes consecutively

drawn without lifting the pen are called a stroke sequence. A PassShape itself may consist of several stroke sequences which may be disconnected shapes.

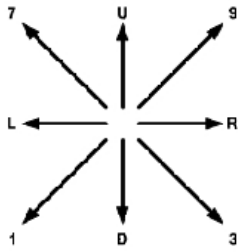

Figure 2: The eight different strokes used in the PassShapes concept

PassShapes can be represented by an alphanumeric string for internal processing and storage. Each stroke has a corresponding character representation as depicted in Figure 2, where the letters indicate the stroke directions: an 'L' stands for 'left', an 'R' stands for right etc. whereas the numbers refer to the direction equivalent to the position of the number on a standard number pad (i.e. '7' corresponds to 'top left'). A pen-up event separating two stroke sequences is marked with an 'X'. An example for internal representation of PassShape is U93DL9L3XU3U. For authentication the user has to reproduce his PassShape either using a touch screen, touch pad or another pointing device. The important aspect is that the strokes of a PassShape are always drawn in the same order, which additionally supports memorability.

The tool based graphical authentication technique is proposed to increase the memorability of passwords[17].This is a well known tool all over the world. M Sreelatha et al[18] proposed shoulder-surfing resistant techniques for PDAs based on images and text. User has to remember pairs of images or pairs of image and text. M Sreelatha et al[19] proposed shoulder-surfing resistant techniques where actual passwords are mapped on to new passwords which makes intruder's task difficult.

3. AUTHENTICATION SCHEME USING "SNAKES AND LADDERS"

Authentication scheme consists of three steps: password registration, password entry and password verification. User creates the password during registration. During login time, user has to enter the password selected by him during registration. Then system verifies the password to authenticate the user. The three important aspects of the password are memorability, usability and security. A good authentication technique should enhance the three aspects.

In order to increase the memorability of passwords, it is proposed to use Snakes and ladders board game. The size of the grid varies from board to board. Most common sizes are 8×8, 10×10 or 12×12. As the board is familiar to all users, the usbility is more. The users are able to remember a sequence of grid cells or ladders or snakes for their password. As they are familiar with the board game , the ladders and snakes it is easy for the users to remember the passwords.

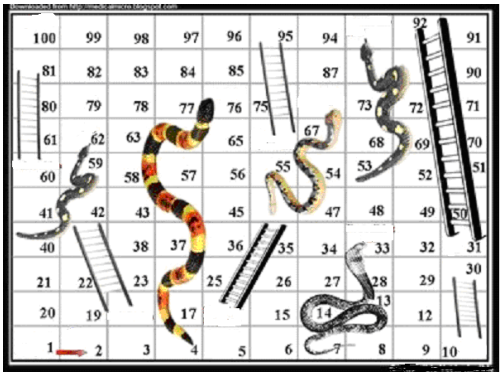

Fig 3: Snakes & ladders

The password can be sequence of three steps i.e. four grid cells in sequence. {18426081} is an example of a password which indicates moves from grid cell 18 to 42, from grid cell 42 to 60 and from grid cell 60 to 81(18→42→60→81). User can select his favorite moves, and enter the grid cells of the sequence of moves as password during registration. During login time, he enters the same sequence as password for authentication. As a numeric value, it is not possible to remember that number. But with the help of board game, it is possible to remember the password.

The advantage of using this tool is no modification is required on the server side. On the client side, this board can be displayed on the screen to help the user to recollect his password.

4. SECURITY ANALYSIS

The Tool is proposed to increase the memorability of passwords. With the help of the tool, it is possible to select lengthy passwords. Lengthy passwords automatically increases the security.

Complexity

Generally the board game consists of 100 cells. For a password with three moves the total password space is 100 x 99 x 98 x 97 theoretically. But, practically the password space may be less than that value. Users may not select all the grid cells with equal priority, they may concentrate only on snakes or ladders. If the user skips all the snakes and considers only ladders for his password, then the password space will be reduced a lot which makes the intruder's task easy. Solution for this problem is to use a game board which is having a picture in each cell. Now the user concentrates not only on snakes or ladders but also the pictures. He can select his favorite pictures and the numbers of those cells can be used for authentication.

Character coding

Instead of cell numbers of the moves, it is possible to use character codes to increase the password space.. The board which we use for password should contain pictures in all cells. Each grid cell is having a picture. User has to select four grid cells for three moves and for the pictures in the grid cells user has to assign some code (2 to 4 characters) which he can recollect by seeing the pictures. During registration, he creates the password by entering the code of all grid cells selected by him in sequence. During login, he enters the password for authentication. Suppose the password contains the moves{46→50→63→66}. The codes are "sari, bila, ramu, sony".

Fig 4: snakes and Ladders with pictures

The story behind these codes is, user assumed for grid cell 46 – "I have a mango color sari", for grid cell 50- "This tree is in the centre of our village bila", for grid cell 63 –" My daughter calls a crow as ramu" and for grid cell 66 – "She looks like my aunty sony". Then the password is "saribilaramusony" which consists of 16 characters. This password is difficult to remember, but with help of game board, it is easy to remember. The password "sariBilaRamuSony" even increases the strength of the password. Characters can be combined with numbers to form alphanumeric password. "sari50ramu66" is an example for alphanumeric password. Special characters can be assigned to some pictures in the grid cells. If the password contains 16 characters, then the password space is 26^{16} for alphabets, 36^{16} for alphanumerics and even more when special symbols are included in the password..

Attacks

Dictionary attack may not be possible because the passwords selected may not be having any meaning and may not be in the dictionary. Exhaustive search attacks may be difficult because of the lengthy passwords. Guessing may be successful if only snakes and ladders are on the board. Are used. If the board contains pictures, then it may be difficult to break the password. Social engineering is also difficult because even user may not be able to remember the password without looking at the board. Though this authentication scheme is vulnerable to shoulder surfing, because of the lengthy password it requires hidden cameras to observe the password.

Shoulder-surfing resistance: The limitation of the technique is shoulder-surfing vulnerability. To make the authentication technique shoulder-surfing resistant , some mapping is required from actual password to some session password. An interface grid will be displayed with 0-9 digits randomly placed in grid cells as shown in fig 5. The number of each cell is to be used to get a digit from the grid. The first digit is used to refer to row and second digit is used to refer to column and the intersecting element becomes part of the password. For an eight password, after mapping a four digit session password can be obtained.

	0	1	2	3	4	5	6	7	8	9
0	9	8	7	5	3	2	1	6	4	0
1	5	4	3	2	7	9	0	8	6	1
2	3	2	4	5	9	0	1	7	8	6
3	1	9	2	8	4	7	3	6	0	5
4	8	6	7	0	1	4	5	9	2	3
5	6	5	4	7	0	8	9	2	3	1
6	2	3	1	4	6	5	8	7	9	0
7	0	1	2	3	4	5	6	7	8	9
8	4	0	9	6	5	3	7	0	1	8
9	7	3	0	9	8	1	4	2	5	6

Fig 5: login interface

Based on the grid cells selected by the user and the interface generated , every time a new session password is entered by the user. For example, for the password {18426781}, the session password is {6770}. The technique reduces the size of the password for digits. The technique is made as shoulder-surfing resistant at the cost of usability and some security.

An alternative method for shoulder-surfing resistance is shown in figure 6. Each two digit number can be mapped on to a two bit number resulting in equal length binary password. For every login , the bits are randomly placed in the grid and it generates a new session password. For an 8 digit password, the session password contains 8 bits and the complexity of finding grid cells is 25^4.

	0	1	2	3	4	5	6	7	8	9
0	00	00	01	10	11	01	10	11	10	00
1	11	01	10	01	10	10	11	01	01	01
2	00	10	11	00	00	11	10	10	11	10
3	10	11	00	10	01	00	01	00	00	11
4	11	00	11	01	00	10	00	11	11	00
5	01	10	00	11	01	11	10	10	01	01
6	00	01	01	00	10	00	11	01	10	10
7	10	11	10	11	11	01	10	00	00	11
8	11	01	00	10	01	10	00	10	01	01
9	10	10	11	01	00	01	01	11	10	10

Fig 6 : login interface with two symbols

5. USER STUDY

User study is conducted with 30 student participants. Initially the participants were asked to select a password of length 6/8/10 digits and enter it on a paper. An even no. of digits password is considered because except the first 9 cells, every grid cell consists of a two digit number and it is easy to map the cells with numbers. First 9 grid cells can be considered as numbers from 00 to 09. The participants are divided into 3 groups to select passwords of different lengths, each group consisting of 10 members. At the end of the first week and the second week, after selecting the password, the participants again entered their password on a paper for verification. The following results were obtained by verifying the passwords with original passwords(table 1). From the results, it is understood that it is difficult to remember lengthy passwords.

Table 1 : Results of memorability study

Length of the password	After first week Memorability	After second week Memorability
6 digits	0.9	0.7
8 digits	0.7	0.6
10 digits	0.5	0.3

An initial session was conducted to explain the scheme and to show the game board to the participants. The game board is displayed on a screen to make them familiar with the game. Then, the participants were informed to select grid cells on the board making moves for his password. In the selection of grid cells, they can have their own story or concept to make moves. Similar to the previous one, participants entered their passwords on a paper. At the end of first and second weeks, after selecting the password the participants entered their password on a paper again, this time with the help of the game board. After verification, it is observed that all participants are able to remember their password (table 2).

Table 2 : Results of memorability study with the help of game board

Length of the password	After first week Memorability(%)	After second week Memorability(%)
6 digits	1.0	1.0
8 digits	1.0	1.0
10 digits	1.0	0.9

After analysis, we observed that the participants concentrated on snakes and ladders only for the selection of password and they are able to remember the password without fail. But with this type of selection, the total password space is reduced. We requested the participants to select character codes for their password and we gave them some time for practice. Later, we repeated the same process and the results are shown in table 3.

Table 3 : Results of memorability study with the help of game board

Length of the password	After first week Memorability(%)	After second week Memorability(%)
3*4 characters	0.9	0.8
4*4 characters	0.8	0.6
5*4 characters	0.7	0.5

The frequency of use has influence on memorability. Most frequently used systems increase the memorability of passwords. In the case of character codes, it is observed that by increasing the frequency of logins, there is lot of improvement in memorability.

The results showed that "Snakes and Ladders" game is a promising tool to increase the memorability of the password. 80% of the participants are interested in game board and 70% of the participants are willing to use the game board as a regular tool. The rest of 80% are ready to use the game board only for lengthy passwords. This indicates the usability of the tool. The remaining 20 % of the participants are not interested in even selecting a lengthy password.

6. CONCLUSION

In general people select short and simple textual passwords to remember them easily. It makes intruder's task easy. Random and lengthy passwords are difficult to remember but provides more security. Graphical passwords are introduced as alternatives to textual passwords. This paper proposed an authentication system which uses "Snakes and ladders" board game to select lengthy and memorable passwords. The board size is generally 10x10 with 100 grid cells. The game consists of number of snakes and ladders. Users can make their favorite moves between grid cells and selects each cell number in the move as part of the password. There is no need to remember the password, user has to remember his favorite moves.

User study is done as paperwork. User study made it clear that the tool has promising results in increasing the memorability of passwords. The usage of well known tool provides usability and the lengthy passwords enhances security. The memorability and usability of character codes should be studied as future work. The user study should be done extensively using systems.

The current study did not concentrate on time requirements. Actually, it is also important that how much time is required to enter a password using the specified tool. It is the future work to find minimum time and maximum time required to enter a password during login.

REFERENCES

[1] Department of Defense Computer Security Center, "Department of Defense Password Management Guideline," Department of Defense, Washington, DC CSC-STD-002-85, April 12 1985.

[2] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password Memorability and Security: Empirical Results," IEEE Privacy & Security, vol. 2, pp. 25-31, 2004.

[3] DTI SURVEY (2006) DTI information security breaches survey. [WWW document] http://www.pwc.co.uk/pdf/pwc_dti-fullsurveyresults06.pdf. GAW S and FELTEN EW (2006) Password management strategies for online.

[4] Davis, D., F. Monrose, and M.K. Reiter. On User Choice in Graphical Password Schemes. 13th USENIX Security Symposium, 2004.

[5] Renaud, K. Evaluating Authentication Mechanisms. Chapter 6 in Cranor, L.F., S. Garfinkel. Security and Usability. O'Reilly Media, 2005.

[6] Nelson, D.L., U.S. Reed, and J.R. Walling. Picture Superiority Effect. Journal of Experimental Psychology: Human Learning and Memory 3, 485-497, 1977.

[7] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

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

[9] D.Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.

[10] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," 21st Annual Computer Security Applications Conference (ASCSAC 2005). Tucson, 2005.

[11] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., "The design and analysis of graphical passwords" in Proceedings of USENIX Security Symposium, August 1999.

[12] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., Memon, N. 2005. PassPoints: Design and longitudinal evaluation of a graphical password system. In: International Journal of Human-Computer Studies (HCI Research in Privacy and Security) 63, 102-127.

[13] J. Goldberg, J. Hagman, V. Sazawal, "Doodling Our Way To Better Authentication", CHI '02 extended abstracts on Human Factors in Computer Systems, 2002.

[14] Sonia Chiasson, P.C. van Oorschot and Robert Biddle, "Graphical Password Authentication Using Cued Click Points".

[15] De Luca, A., Weiss, R., Drewes, H. Evaluation of Eye-Gaze Interaction methods for Security Enhanced PIN-Entry. In: Proceedings of OZCHI 2007, Adelaide, Australia, 28 – 30.11.2007.

[16] A. D. Luca, R. Weiss, and H. Hussmann, "PassShape : stroke based shape passwords," in Proceedings of the conference of the computer-human interaction special interest group (CHISIG) of Australia on Computer-human interaction: design: activities, artifacts and environments. 28-30 November 2007, Adelaide, Australia, pp. 239-240.

[17] Sreelatha Malempati and Shashi Mogalla, "A well known tool based Graphical Authentication technique", CCSEA 2011, CS & IT 02, pp. 97-104, DOI : 10.5121/csit.2011.1211

[18] M Sreelatha, M Shashi, M Anirudh, Md Sultan Ahamer, V Manoj Kumar, "Authentication Schemes for session passwords using color and images", IJNSA Vol.3, No.3, May 2011, DOI : 10.5121/ijnsa.2011.3308