Global Journal of Computer Science and Technology: C
Software & Data Engineering
Volume 17 Issue 3 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Shoulder Surfing Resistant Graphical Authentication Scheme for Web based Applications

By Seun Ebiesuwa, Ariweriokuma, P.E, & Akinsanya, Adebola

Babcock University

Abstract- Since the design and development of the first graphical authentication pioneered by Blonder in 1996, numerous research has been conducted on this area to be used in different scenarios especially on the Internet. One of the major motivators is the picture superiority which as studies have shown, states that images/pictures provide higher memorability as opposed to Text based authentication. However, graphical authentication is still faced with some challenges. In this paper, a shoulder surfing resistant graphical authentication scheme is proposed to tackle a major issue related to the graphical authentication schemes developed. The proposed scheme provides a high level of resistance to shoulder surfing attacks, mitigating the need to upload pictures and aids in finding chosen objects in the scheme.

Keywords: authentication, text-based authentication, graphical based authentication, security, shoulder surfing.

GJCST-C Classification: D.2.6, H.5.2

Shoulder Surfing Resistant Graphical Authentication Scheme for Web based Applications

Seun Ebiesuwa [α], Ariweriokuma, P.E.[σ], & Akinsanya, Adebola [ρ]

Abstract- Since the design and development of the first graphical authentication pioneered by Blonder in 1996, numerous research has been conducted on this area to be used in different scenarios especially on the Internet. One of the major motivators is the picture superiority which as studies have shown, states that images/pictures provide higher memorability as opposed to Text based authentication. However, graphical authentication is still faced with some challenges. In this paper, a shoulder surfing resistant graphical authentication scheme is proposed to tackle a major issue related to the graphical authentication schemes developed. The proposed scheme provides a high level of resistance to shoulder surfing attacks, mitigating the need to upload pictures and aids in finding chosen objects in the scheme. However, the schemes has some vulnerabilities which implies that there may not be a perfect graphical authentication scheme; each scheme has its merits and demerits making it a suitable candidate for different environment and/or event depending on its architecture.

Keywords: authentication, text-based authentication, graphical based authentication, security, shoulder surfing.

I. Introduction

Graphical based authentication is a type of knowledge based authentication which uses images/picture to assist users in generating a more robust password (Suo, Zhu & Owen, 2005). Due to its picture superiority which according to Paivio in 1991, pictures are dually encoded and this is an advantage over words. While words are merely encoded verbally, pictures produce both a verbal code and an image code because participants are more likely to hold a label for pictures than to imagine words. Having two types of codes tagged to the pictures allow a greater chance of retrieval during a memory task (Paivio 1991). In addition, classic cognitive science experiment conducted have shown that humans have a strong memory ability for images. The experiment showed a recognition performance exceeding 90%, indicating retention of over 2,000 items, even when up to 3 days elapsed between learning and testing (Standing, Conezio, & Haber, 1970).

The challenge of users generating weak guessable passwords in text based authentication has been one of the major reasons numerous research has been conducted on Graphical based authentication (Prakash, Infant & Shobana, 2010). The concept of Graphical based authentication is creating a level of abstraction whereby users do not actually know the set of password characters generated but a pattern used in generating the passwords. However, over the years, Graphical based authentication schemes have been faced with numerous challenges including vulnerability to shoulder surfing attacks, the size of pictures used and browsing through an array of images/objects without assistance(Biddle, Chiasson & Oorschot, 2011; Wiedenbeck, Waters, Birget, Brodskiy & Memon, 2005). The proposed Graphical authentication schemes reviewed in this paper tackles majorly on the above-mentioned issues.

The rest of the paper is structured as follows: a brief overview of Graphical based authentication and it techniques; examples of the schemes that utilize the techniques of Graphical based authentication, listing their features, pros and cons; the proposed scheme and its architecture; summary and conclusion.

II. Graphical based Authentication

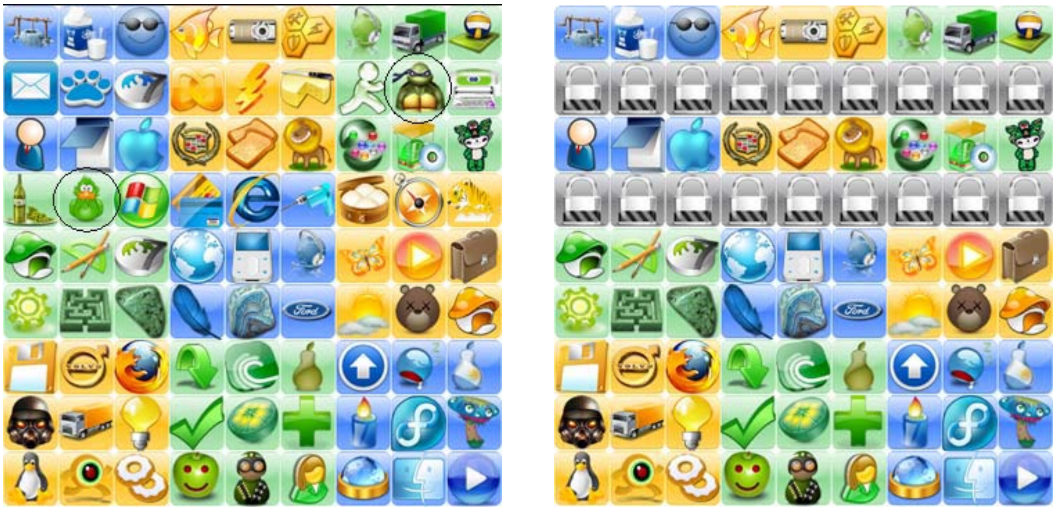
Graphical based password authentication is a type of knowledge based authentication that uses images or pictures in verifying the identity of a user. It is categorized generally into the following: recognition-based, recall-based and cued recall techniques (Suo et al, 2005). Based on the various techniques, the steps for both registration and authentication varies.

a) *Recognition-Based technique*

This involves the recognition and selection of a set (usually a fraction of the main set) of pre-selected objects (usually images) from a portfolio of objects. One scheme that utilize this technique is as follows:

Author α σ ρ: School of Computing and Engineering Sciences Babcock University, Ilishan, Ogun State, Nigeria. e-mail: seunebi@gmail.com

i. *Colorlogin*



Source: Gao, Liu, Wang and Dai(2009)

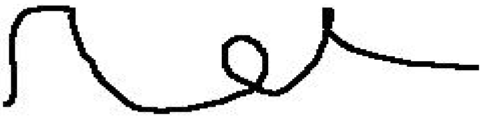
Figure 1.0: Colorlogin

ColorLogin by Gao et al utilizes recognition based technique involving choosing multiple icons as password icons or pass-icons (Shown in Figure 1.0). The background of every icon belongs to one of the finite set of colors given. Registration involves choosing a color which then displays all the set of icons whose background color is the same as the chosen color. Users are required to choose 3 icons from the set of icons displayed. During authentication, icons of different background colors including 2 of the user's icons will be randomly displayed on a grid. Users only need to select the row where the pass icon is located (no need to click on the icon itself but any other icon on the same row with it) and after which all the icons on that row will be substituted with a lock icon. A user is authenticated after getting the pass icon in one attempt else the icons will be shuffled for the user to try again. Using of colors and selecting of row improves the security against shoulder surfers. In this authentication, some icons are frequently chosen as pass icons creating so-called hotspots and also searching through an array of icons can become tiring for the user.

b) Recall-based or Pure recall technique

This requires the user to reproduce something that was created during registration; example includes:

i. *Passdoodle*



Source: Varenhorst, Kleek and Rudolph(2004)

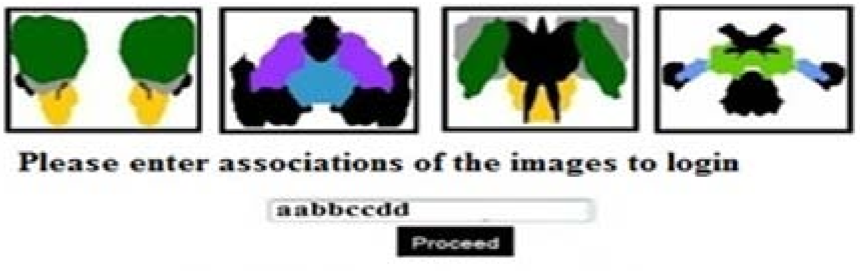
Figure 1.1: Passdoodle

Varenhorst et aldeveloped Pass-doodles in 2004 using recall based technique. It is a hand-written design usually drawn with stylus unto touch sensitive screen. A doodle in this case is an ordered set of points which is drawn (Figure 1.1 is an example of a doodle) and saved during registration. In addition to the doodle drawn, the speed used in drawing the doodle is also calculated and saved. This graphical authentication scheme provides an easy way for users to remember the pass-doodle drawn but it was observed that sometimes the users forget the order in which they were drawn and also it tends to be vulnerable to shoulder surfing.

c) Cued recall technique

Cued recall assist the user by providing a cue (a clue or hint) to enable the user recall from memory and reproduce the information that was created during registration. The following ae some examples:

i. *Passbolt*



Please enter associations of the images to login

aabbccdd

Figure 1.2: Passblot login screen

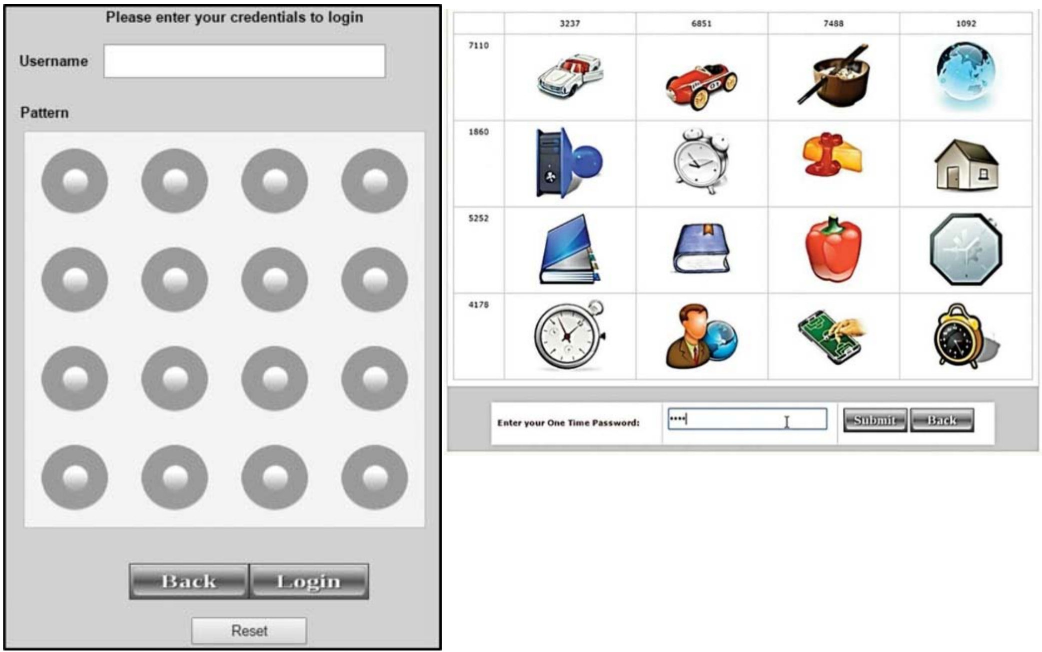
Source: Gupta, Sahni, Sabbu, Varma and Gangashetty(2012)

Developed by Gupta et al in 2012, Passblot is a graphical One-Time Password (OTP) that uses cued recall technique. The authentication performs an inkblot test, a psychological evaluation to get the users unique description of an image (Carlson & Heth, 2010). Figure 1.2 describes Passblot authentication. On registration, a given set of inkblots images are displayed; the first and last letter of the description of each inkblot is saved (i.e. if a user's description for a particular inkblot is "butterfly" then "by" is saved or if the description is "standing man" then "sn" is saved). All the displayed inkblots images have to be described and saved for that particular user. Upon authentication, a fraction of randomly chosen inkblot images from the user's set will be displayed for the user to describe. By randomly selecting a fraction of the users set of pictures upon login gives a dynamic password creating a probabilistic situation for dictionary attack and brute force. Nevertheless, in other for the module to be properly secured a large amount of inkblot pictures is required which is a load for the server and can be tiring for the user on registration and authentication.

d) *Hybrid technique*

Over the years, in attempt to provide a more secured graphical authentication system, combinations of these techniques have been implemented. Examples of such systems includes:

i. *Graphical One Time Password*



Please enter your credentials to login

Username

Pattern

Enter your One Time Password: ****

Source: Alsaiari, Papadaki, Dowland and Furnell (2016)

Figure 1.3: Graphical One Time Password

In 2016, Alsaiari et al developed Graphical One Time Password (GOTP) and as the name implies implements One-Time Password (OTP) mechanism for additional security. From Figure 1.3, this is a combination of three authentication mechanisms which includes a 4x4 grid lock pattern (recall-based), identification of pass image (recognition-based) and finally inputting an OTP corresponding to the chosen/identified images. The right OTP will be associated with the correct images and it is also a challenge from the server. On registration, a lock pattern is drawn and a set of four (4) images out of thirty (30) are chosen. During authentication, the user first begins by drawing the lock pattern, next to selecting the right images (two of the previously selected four) from the portfolio of images and finally inputting a random number (i.e. one-time password if the right one is chosen) associated with the selected images. This will be sent as a response to the server. This authentication improves the ability to recall the pattern and identify images more efficiently. Nevertheless, a reasonable amount of pictures need to be stored on the server for improved security which can be a bottle neck for the server.

III. Limitations of Reviewed Works

From the works reviewed, many of the graphical authentication models developed are susceptible to shoulder attack which has been found to be one of the major challenges. The few which are not susceptible require a search through an array of objects which can be demanding for the user and/or require a reasonable number of pictures (with lots of details) to be made secured which can be demanding in storing such unique images for different users creating a burden for the server. Therefore, there is a need for a shoulder surfing resistant graphical authentication for web applications which should require little number of images and little time to generate the graphical password.

IV. Proposed Scheme

This scheme utilizes set of colored rows and columns which may assist users in identifying their chosen cell. The interface design elaborates on the cued recall graphical technique being utilized. This scheme will involve the following;

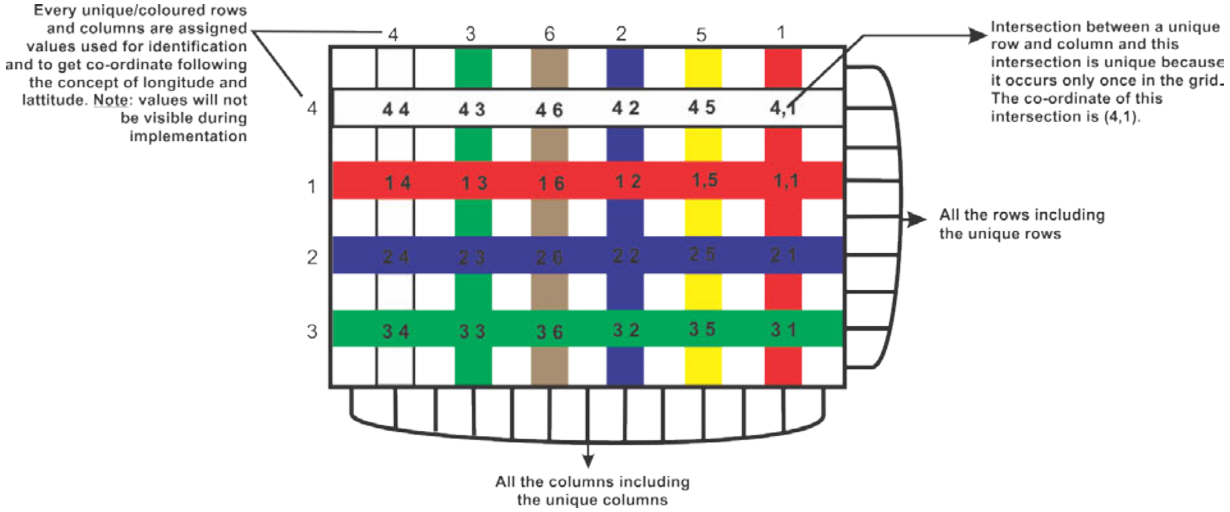
i. *Rows and Columns:* As shown in Figure 1.4, the grid is made of 13 columns and 9 rows. From these rows and columns are 6 columns and 4 rows that are assigned unique colours and values (these are all the even rows and columns; the odd rows and column are not assigned any colour or value). The values are permanently assigned to the rows and columns. The concept of these unique rows, columns and their intersection is gotten from the earth's longitude and latitude whose intersection is unique and are used to provide co-ordinates. (The Editors of Encyclopedia Britannica, 2012). Every intersection of the coloured rows and column is unique and its purpose is to assist in locating a particular cell in the grid. Figure 3.1, shows the intersection between the white row (4) and red column (1); the format of this co-ordinate is written as (4,1). During registration and authentication, these coloured rows and columns are randomly arranged on the grid but still retain the values given to them.

Table 1.0: Colored columns and their associative value

Color	Value
Red	1
Blue	2
Green	3
White	4
Yellow	5
Brown	6

Table 1.1: Colored rows and their associative value

Color	Value
Red	1
Blue	2
Green	3
White	4



Every unique/coloured rows and columns are assigned values used for identification and to get co-ordinate following the concept of longitude and lattitude. Note: values will not be visible during implementation

Intersection between a unique row and column and this intersection is unique because it occurs only once in the grid. The co-ordinate of this intersection is (4,1).

All the rows including the unique rows

All the columns including the unique columns

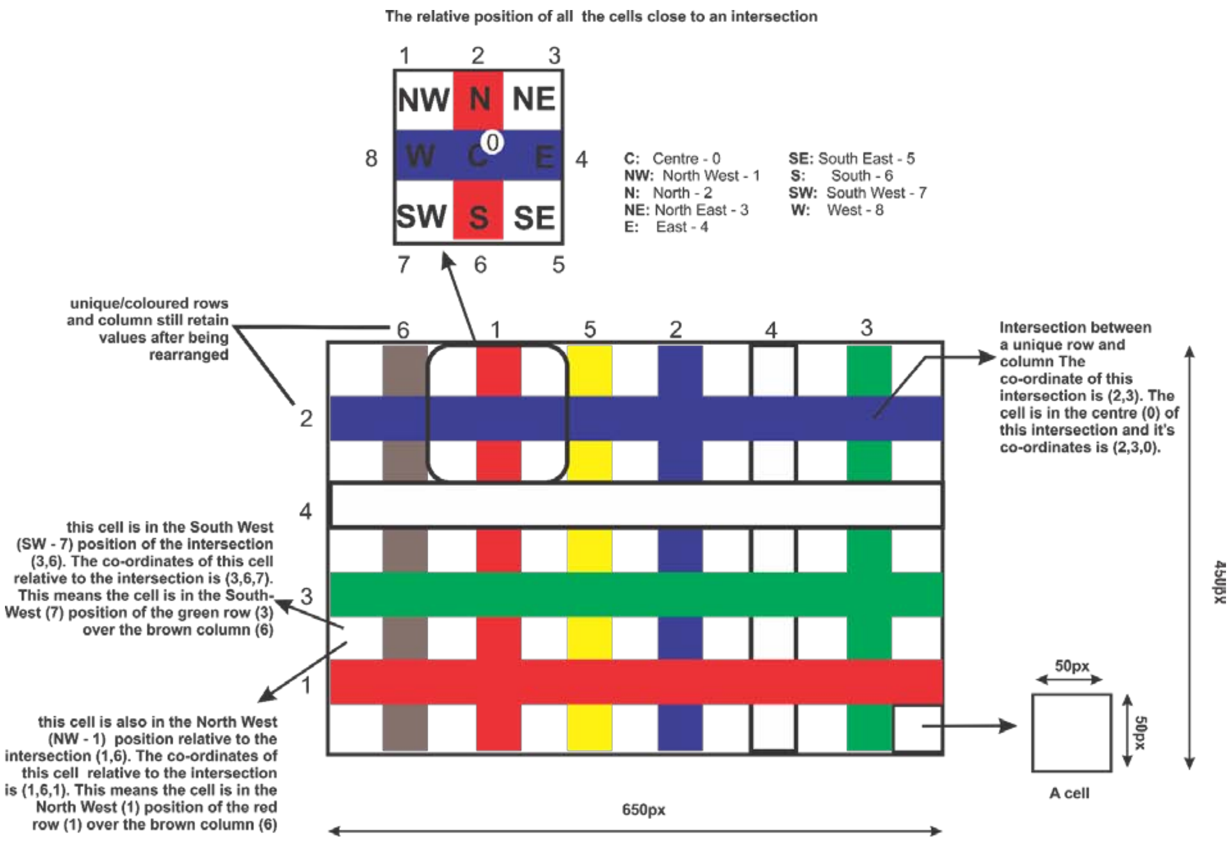
Figure 1.4: Unique rows, columns and their intersections

The position/location of every cell in the grid is relative to their neighbouring intersection as shown in Figure 1.5 (i.e. the cardinal points of the intersection). Each cell contains two values (integers between 0 and 9). The first value (or left value) and the second value (or right value). These values are different from the values assigned to each line.

ii. *Cells:* There are a total number of 117 cells in the grid. Each cell in the grid has a width and height of 50pixels each giving the grid a total area of 650 by 450 pixels. The position/co-ordinates of each cell is relative to the individual intersections closest to them. As shown in Figure 1.5, A cell can be in the North, North West, North East, East, South East, South West, South, West or at the centre of an intersection. All these positions are assigned values and are used in identifying the position/co-ordinates of a cell based on the unique intersection chosen.

Table 1.2: Cardinal Points and their associative values

Position	Value
Centre	0
North	1
North East	2
East	3
South	4
South West	5
West	6
North West	7



unique/coloured rows and column still retain values after being rearranged

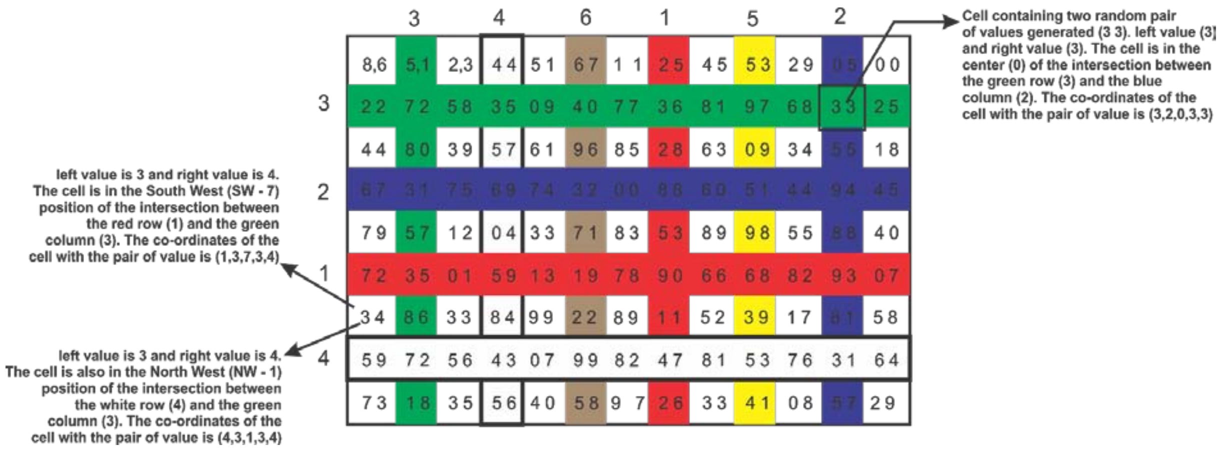
Intersection between a unique row and column The co-ordinate of this intersection is (2,3). The cell is in the centre (0) of this intersection and it's co-ordinates is (2,3,0).

this cell is in the South West (SW - 7) position of the intersection (3,6). The co-ordinates of this cell relative to the intersection is (3,6,7). This means the cell is in the South-West (7) position of the green row (3) over the brown column (6)

this cell is also in the North West (NW - 1) position relative to the intersection (1,6). The co-ordinates of this cell relative to the intersection is (1,6,1). This means the cell is in the North West (1) position of the red row (1) over the brown column (6)

Figure 1.5: Cells and their co-ordinates

Co-ordinates of several cells are shown in Figure 1.5. One of which is the cell at the South West (SW - 7) position of the intersection between the green row (3) and brown column (6) and this co-ordinate is written as (3,6,7).



		3		4		6		1		5		2	
	8,6	5,1	2,3	44	51	67	1 1	25	45	53	29	05	00
3	22	72	58	35	09	40	77	36	81	97	68	33	25
	44	80	39	57	61	96	85	28	63	09	34	56	18
2	67	31	75	69	74	32	00	88	60	51	44	94	45
	79	57	12	04	33	71	83	53	89	98	55	88	40
1	72	35	01	59	13	19	78	90	66	68	82	93	07
	34	86	33	84	99	22	89	11	52	39	17	81	58
4	59	72	56	43	07	99	82	47	81	53	76	31	64
	73	18	35	56	40	58	9 7	26	33	41	08	57	29

Cell containing two random pair of values generated (3 3). left value (3] and right value (3). The cell is in the center (0) of the intersection between the green row (3) and the blue column (2). The co-ordinates of the cell with the pair of value is (3,2,0,3,3)

left value is 3 and right value is 4. The cell is in the South West (SW - 7) position of the intersection between the red row (1) and the green column (3). The co-ordinates of the cell with the pair of value is (1,3,7,3,4)

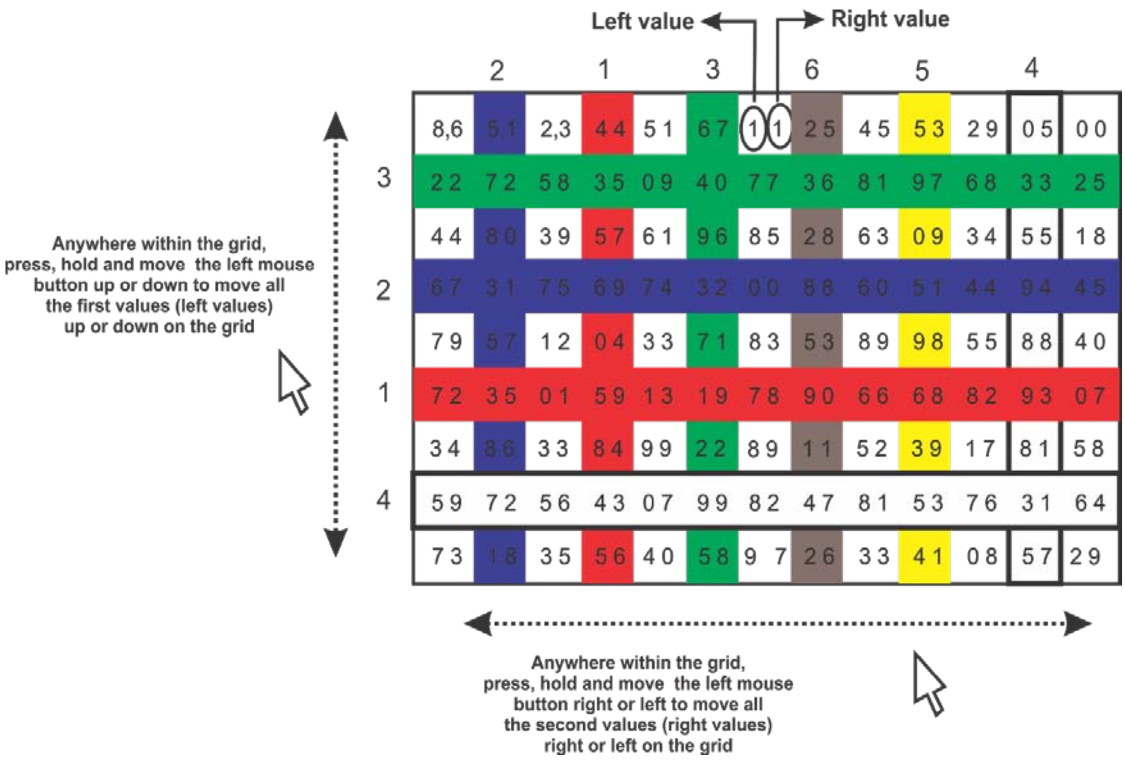
left value is 3 and right value is 4. The cell is also in the North West (NW - 1) position of the intersection between the white row (4) and the green column (3). The co-ordinates of the cell with the pair of value is (4,3,1,3,4)

Figure 1.6: The grid populated with pair of values in each cell

Figure 1.6 shows the complete interface used for the scheme. Each cell contains a pair of value; a right and a left. These pair of values are randomly generated between 0 and 9 using JavaScript and it is done during registration and authentication. As shown in Figure 1.6, one of the co-ordinates of a cell and the values it contains includes: the value of the green row (3), value of the blue column (2), the position of the cell relative to the intersection of the chosen row and column (which in this example is the centre - 0), the left value in the cell (3) and the right value in the cell (3) and this is written as (3,2,0,3,3). This forms the complete graphical password and will be stored in the database during registration and be generated during authentication.

ii. *Inserting values into the cells:* In this scheme, the use of the keyboard to inserts the desired pair of values (i.e. left and right values) is not allowed. In other to insert values, the user makes use of only the mouse. As shown in Figure 1.7, values are moved about from one cell to another either from left to right (or vice visa) or up to down (or vice visa).

This is done by pressing, holding and moving the left mouse button anywhere within the grid. Moving the mouse left or right will affect all the right values in the cell causing them to move from one cell to another either to the left or right position. On the other hand, moving the mouse up or down will affect all the left values in the cell causing them to move from one cell to another either upwards or downwards. For cells located at the edge of the grid, new randomly generated values will be moved into the cell.



		2		1		3		6		5		4	
	8,6	5,1	2,3	44	51	67	11	25	45	53	29	05	00
3	22	72	58	35	09	40	77	36	81	97	68	33	25
	44	80	39	57	61	96	85	28	63	09	34	55	18
2	67	31	75	69	74	32	00	88	60	51	44	94	45
	79	57	12	04	33	71	83	53	89	98	55	88	40
1	72	35	01	59	13	19	78	90	66	68	82	93	07
	34	86	33	84	99	22	89	11	52	39	17	81	58
4	59	72	56	43	07	99	82	47	81	53	76	31	64
	73	18	35	56	40	58	9 7	26	33	41	08	57	29

Anywhere within the grid,
press, hold and move the left mouse
button up or down to move all
the first values (left values)
up or down on the grid

Anywhere within the grid,
press, hold and move the left mouse
button right or left to move all
the second values (right values)
right or left on the grid

Figure 1.7: Moving values in the cell within the grid

a) Creating/Setting up a graphical password

This section explains the steps for creating/setting up a graphical password. These steps are explained as follows:

i. Select one coloured row.
ii. Select one coloured column.
iii. Select a cell whose location is relative to the intersection of the chosen row and column (i.e. a cell North, South, South-East, South-West, North-East, North West, West or East of the intersection).
iv. Press and drag the left mouse button up or down within the grid to move a desired value into the first side (left side) of the chosen cell.
v. Press and drag the left mouse button left or right within the grid to move a desired value into the second side (right side) of the chosen cell.

Here the password created will be (in this order), the value of the chosen row, the value of the chosen column, the position (in value) of the cell relative to the intersection, the chosen value for the first side (left side) and second side (right side) of the chosen cell. The format is written as (R,C,P,Le,Ri) Where:

R = the value of the row chosen, 1<=R<=4.
C = the value of the column chosen, 1<=C<=6.
P = the position of the cell to the intersection of the chosen R and C, 0<=P<=8.
Le = the left value of the chosen cell, 0<=Le<=9 and
Ri = the right value of the chosen cell, 0<=Ri<=9.

The co-ordinates includes (R,C,P) which identifies the users chosen cell, while (Le,Ri) are the pair of values found in those co-ordinates (chosen cell). The graphical password includes the combination of the co-ordinates and the pair values which will be stored in the database. The co-ordinates will also be stored in the database to enable the authentication scheme know the users chosen cell in other to retrieve the inputted pair of value. The co-ordinates will be used for authentication.

b) Generating a Graphical Password

This section explains the steps for generating a graphical password after creating/setting up a password. In this phase, the co-ordinates stored for the registered user is utilized in other to know the user's chosen cell and acquire the pair of values in that cell.

Every time during this phase, the order/arrangement of the unique rows and columns are randomly placed, only the user knows his/her chosen row, column, position (co-ordinates) and the pair of values to be inserted in to the chosen cell. This phase includes the following:

i. By pressing and dragging the left mouse button up or down within the grid, assign the pre-chosen value for the first side (left side) into the chosen cell.

ii. By pressing and dragging the left mouse button left or right within the grid, assign the pre-chosen value for the second side (right side) into the chosen.

iii. Proceeding to the next phase the authentication scheme only validates the values located at the chosen cell as the scheme already knows the chosen cell.

c) System Development Tools

Selection of appropriate system development tools is required to provide a robust, reliable and effective graphical authentication system. These tools include.

1. *HTML (Hyper Text Mark-up Language)*: This is a mark-up language that is used to create and design the structure of the scheme. To achieve the grid system made of 117 cells, a table tag is created containing 9 table row tags which in turn contains 13 table definition tags each. Each table definition (a cell) contain a unique identity.
2. *CSS (Cascading Style Sheets):* This is used for presentation and in this scheme, provides each selected row and column its unique colour and styling.
3. *JavaScript:* It plays a major role in this research as it is responsible for interacting with the user. This performs the client side scripting and used for the development of the graphical interface for creating/setting up and generating password. In this project, it will be performed both at the frontend framework and backend framework.
4. *WAMP Package:* The acronym WAMP stands for Windows Apache MySQL PHP and it is a software suite designed specifically for Windows operating system. This suite creates a sandbox for the development of web based application which provides four key elements: An operating system, database, web server and a scripting software.

Apache is the web server used to execute the different codes presented. MySQL is the type of database used during this project. PHP (PHP Hypertext Pre-processor) performs at the backend, this is used to connect to the database and serve as the server scripting language.

5. *PhpMyAdmin:* This is a friendly interface used to manage the activities of the database.

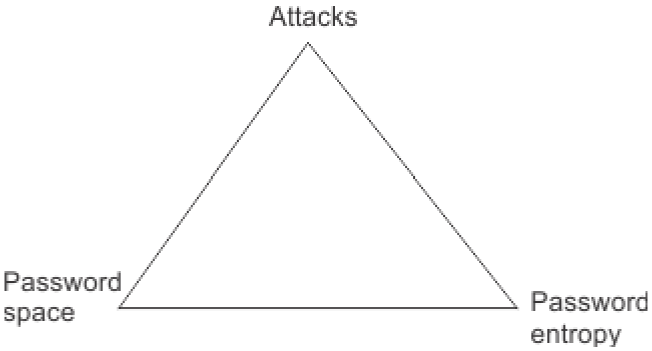
V. Features of the Proposed Scheme

The architecture of the scheme provides different features to tackle the issues associated with reviewed existing graphical schemes. These features include.

1. *Shoulder surfing resistance:* Firstly, during the process of inputting the chosen values into the chosen cells, every other value is affected and move simultaneously according to the movement of the mouse. Secondly, during every authentication, the coloured rows and column are randomly placed making the scheme dynamic. These feature screate a level of resistance to shoulder surfing attacks.
2. *Optimization of storage capacity:* The use of HTML (Hyper Text Mark-up Language), CSS (Cascading Style Sheet) and JavaScript creates a dynamic table where the coloured rows and columns are rearranged during authentication. This dynamic grid system is used as the image for authentication thereby mitigating the need for picture uploads and/or storage.
3. Assistance in finding objects: The coloured rows and columns provides assistance for users to locate the chosen cell for inputting the chosen pair of objects. Rather than searching through each cell, user focus on their chosen coloured row and column. This streamlines the search.

VI. Evaluation of the Scheme

Using magic triangle evaluation, an evaluation scheme designed by Lashkari, Manaf, Masrom, and Daud in 2011 which shows 3 attributes of security in Graphical authentication.



Source: Lashkari et al (2011)

Figure 1.8: Magic triangle for Graphical Authentication security evaluation

The password space and entropy was calculated using

$$\text{SPACE} = M^N$$

Where:

M = is the number of characters and

N = is the length of the password (Lashkari et al, 2011).

For password space and

Entropy = $N\log_2(|L||O||C|)$

Where

N = the length or number of runs,

L = locus alphabet as the set of all loci

O = is an object alphabet and

C = color of the alphabet (Zhu, Qibin, Yong, & Giusto, 2005).

The password space and entropy were shown to be $2.61*10^4$ and 14.39 respectively. These results are very low making it susceptible to brute force attacks, therefore, an additional security feature should be added to this scheme against such attacks.

VII. Limitation

Several researches have been conducted on Graphical based authentication schemes, however, this area is still in its infancy. In this scheme, the security issues tackled were majorly on shoulder surfing; other areas such as usability were not properly addressed.

VIII. Conclusion

From the different scheme reviewed, there has not been a perfect Graphical authentication scheme for all scenario. Every graphical authentication has its pros and cons suitable for specific scenario. Before utilizing any graphical scheme, a proper analysis should be conducted to determine the best scheme that will be appropriate.

References Références Referencias

1. Alsaiari, H., Papadaki, M., Dowland, P., & Furnell, S. (2016). Graphical One-Time Password (GOTPass): A usability evaluation. *Information Security Journal: A Global Perspective*. doi:10.1080/19393555.2016.1179374
2. Biddle, R., Chiasson, S., & Oorschot, P. (2011). *Graphical password: Learning from the first twelve years.* Technical Report TR-11-01,.
3. Carlson, N. R., & Heth, D. C. (2010). Psychology--the science of behaviour. Toronto: Person.
4. Gao, H., Liu, X., Wang, S., & Dai, R. (2009). Design and Analysis of a Graphical Password Scheme. *Innovative Computing, Information and Control (ICICIC).* IEEE Xplore. doi:10.1109/ICICIC.2009.158
5. Gupta, S., Sahni, S., Sabbu, P., Varma, S., & Gangashetty, S. V. (2012). Passblot: A Highly Scalable Graphical One Time Password System. *International Journal of Network Security & Its Applications (IJNSA), 4*(2).
6. Lashkari, A. H., Manaf, A. A., Masrom, M., & Daud, M. S. (2011). Security Evaluation for Graphical Password. *International Conference, DICTAP 2011, Proceedings, Part I.166*, pp. 431-444. Dijion, France: Springer Heidelberg Dordrecht.
7. Paivio, A. (1991). Dual coding theory: Retrospect and current status. *Canadian Journal of Psychology*(45), 255-287.
8. Prakash, M. V., Infant, P. A., & Shobana, S. J. (2010). Eliminating Vulnerable Attacks Using One-Time Password and PassText – Analytical Study of Blended Schema. *Universal Journal of Computer Science and Engineering Technology, 1 (2)*, 133-140.
9. Standing, L., Conezio, J., & Haber, R. N. (1970). Perception and memory for pictures: Single-trial learning of 2500 visual stimuli. *Psychonomic Science, 19(2)*, 73–74. doi:DOI: 10.3758/BF03337426
10. Suo, X., Zhu, Y., & Owen, S. G. (2005). Graphical Passwords: A Survey.
11. The Editors of Encyclopedia Britannica. (2012, July 3). *Latitude and longitude*. Retrieved April 5, 2017, from Encyclopedia Britannica: https://www.britannica.com/science/latitude
12. Varenhorst, C., Kleek, V. M., & Rudolph, L. (2004). Passdoodles; a Lightweight Authentication Method. *Research Science Institute*.
13. Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., & Memon, N. (2005). PassPoints: design and longitudinal evaluation of a graphical password system. *Int. J. Hum.-Comput. Stud. 63, 1-2*, 102-127.

This page is intentionally left blank