International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Graphical Password Knowledge Based Authentication System Enhancement Using Persuasive Technology

Prof. Uma Yadav[1], Sarita Sakure[2]

[1]Department of Computer Science & Engineering, Shri. Ramdeobaba College of Engineering and Management, Nagpur, India

[2]Professor, Department of Computer Science & Engineering, Dr. Babasaheb Ambedkar College of Engineering and Research, Nagpur, India

Abstract: ***An Existing authentication system has certain drawbacks which results now a day's graphical passwords are most preferable authentication system where users click on images to authenticate themselves. An important aspect of an authentication system is to support users for selecting the better password. Basically user creates most memorable password which is easy to guess by an attacker and system assigned passwords are difficult to memorize. So researchers of modern days gone through different alternative methods and conclude that graphical passwords are most preferable authentication system. The proposed system combines the existing cued click point technique with the persuasive feature to influence user choice, encouraging user to select more random click point which is difficult to guess.***

Keywords: Authentication, Graphical Password, images, Usability, Security.

1. Introduction

The problem of Knowledge based authentication typically text based password are well known. The goal of an authentication system is to support users in selecting the better password. An alternative option to alphanumeric password is the graphical password. Graphical password uses images or part of an image as a password. Human brains easily recognize pictures better than the text. Most of the time user create memorable password which is easily guess by an attacker whereas system assigned password are difficult to remember. [1][2] An authentication system should allow user choice while influencing user towards stronger passwords. An important usability goal of Knowledge based authentication system is to support users in selecting password of higher security with larger password space. Basically persuasion is used to control user choice in click based graphical password, encouraging user to select more random click point which is difficult to guess. In the proposed system, the task of selecting weak password which is easy for an attacker to guess is more tedious, discourage users from making such choices. In consequence, this approach chooses the more secure password the path of least confrontation. Instead of placing the burden on users it's easier to track the system suggestions for a secure password which is the feature lacking in most of the schemes. Here persuasive feature is combined with previous cued click point technique [9] which uses one click point on five different images. The next image to be displayed is based on previous click-point and the user specific random value. Here the password entry becomes a true cued recall scenario wherein each image triggers the memory of corresponding click-point. For valid users it provides implicit feedback such that while logging if user unable to recognize the image then it automatically alters the user that their previous click-point is incorrect and user can restart the password entry where as explicit indication is provided after the final click point.

2. Classification of Authentication Methods

The following figure 1 shows the classification of different authentication methods. Biometric based authentication techniques are somewhat expensive, slow and unreliable and most of the time it not recognizes the people and thus not preferred by many [4]. Token based authentication system has high security and usability and accessibility then the others. Also the system uses the knowledge based techniques to enhance the security of token based system. But the problem with token based system is that if token get lost, the security get also lost [3].

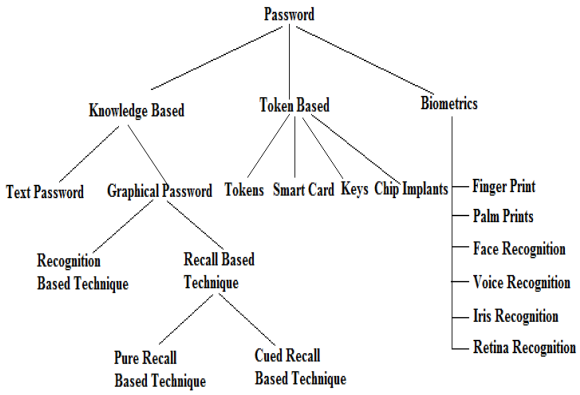

Figure 1: Classification of Password Authentication Techniques

Therefore the Knowledge based authentication techniques are most preferable technique to improve the real high security. Graphical Password is one of the knowledge based technique and it is categorized into Recognition based and Recall based [12].

Licensed Under Creative Commons Attribution CC BY

3. Literature Review

G. E. Blonder [5] proposed graphical password scheme in which user click on several different predefined location on a predetermined image. During login, the user has to click on the approximate area of those locations. Basically the image helps the user to call upon their passwords and therefore this scheme is considered more suitable than unassisted recall. The problem with this system is that boundaries are predefined which results various attacks are easily possible.

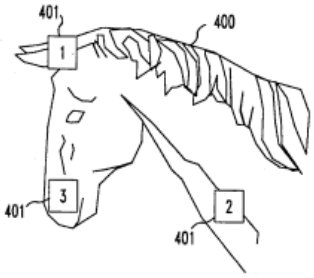

Figure 2: Blonder's Scheme

S. Wiedenbeck et al. [6][7][8] proposed pass-point graphical password scheme in which password consists of a sequence of 5 different click point on a given image. During password creation user can select any pixel in the image as a click-points and during authentication the user has to repeat the same sequence of clicks in correct order within a system defined tolerance square of original click-points. Pass-point used the robust discreatization technique. The problem with this scheme is that HOTSPOT (area of an image where user more likely to select the click-point) and also user makes certain kinds of patterns in order to remember the password which means pattern formation attacks are easily possible.

Figure 3: Pass-Point

S. Chaisson et al. [9] proposed cued click -point which was intended to reduce the HOTSPOT and pattern formation attack. CCP uses one click point on five different images instead of five click-points on one image. The next image to be displayed is based on previous click-point and the user specific random value by using a deterministic function. Here the password entry becomes a true cued recall scenario wherein each image triggers the memory of corresponding click-point. For legitimate users it provides implicit feedback such that while logging if user unable to recognize the image then it automatically alters the user that their previous click-point is incorrect and user can restart the password entry where as explicit indication is provided after the final click point. CCP also used the robust discreatization technique. The problem with this technique is false accept and false reject is possible.

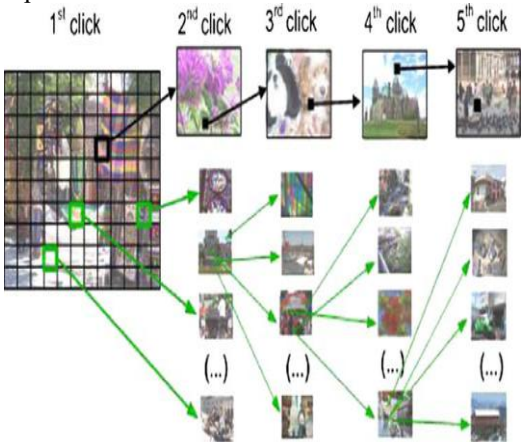

Figure 4: Cued Click point

A. Forget et al. [11] proposed persuasive text password (PTP) scheme which employs a persuasive technology principles to persuade users in creating more secure passwords. During password creation, the user select his own password, the PTP improve its security by placing the arbitrary chosen characters at random positions into the password. Users can shuffle the random characters until they find the combination to be memorable. Basically PTP is a user-chosen text secret code system which helps user to build their password more secure.

4. Proposed System

The proposed system is based on click based graphical password system that not only guides and helps the user for password selection but also encourages the user to select more random distributed password. The proposed system is based on Persuasive Technology which motivates and influence people to behave in a desired manner [10]. The proposed system combines the Persuasive features with the cued click-point to make authentication system more secure. Basically during password creation the part of an image which is less guessable is highlighted and user has to select the click-point within the highlighted portion and if the user is unable to select the click-point then he can move towards the next highlighted portion by pressing the shuffle button. The highlighted part of an image basically guides users to select more random passwords that are less likely to include hotspots. Therefore this works encouraging users to select more random, and difficult passwords to guess. During Login, images are displayed normally and user has to select the click-point as chosen at the time of password creation but this time highlighted portion is not present as it only provides the system suggestion. An important usability goal of proposed system is to support users in selecting password of higher security with larger password space. The proposed system removes the pattern formation attack and Hotspot attack (it is an area of an image where most of the user is selecting it as the click-point).Also it removes the shoulder surfing attack. Also the present system deals with variable number of click point where user has a choice to define the

Licensed Under Creative Commons Attribution CC BY

length of the password such as he or she may choose 3 click-points, 5 click-points and 7 click-points as a password length.

5. Analysis of Algorithms

The proposed system is implemented and it has used following algorithms

5.1 Seed Generation Algorithm

This algorithm is used to set the seed value or unique value for the user. This seed value plays a vital role to select the First image. Also this seed value is used for further image selection. The seed value is generating on the basis of user name. Then the user name and seed value will decide the First image. Here for example such that user name is "uma.yadav12@gmail.com" and for this user name the seed value generated is "65023" and correspondingly first image is retrieve on the basis of user name and seed value.

5.2 Centred Descreatization Algorithm

Discreatization is used to just allow the correct click-points to be accepted in the region without storing exact click-point co-ordinates. Centred Descreatization [13] offers centre tolerance such that during password creation an invisible grid is overlaid in such a way that the grid comes in centre with respect to selected click-point and the grid size used is 2r×2r. It divides an image into square\ tolerance regions, to verify whether a login click-point comes within the same tolerance region as the original click-point. During password creation the grid's location is set for every click-point and there is a identical tolerance area centered around the original click-point, by calculating the appropriate (x,y) and grid offset (Gx,Gy) (in pixels) from a (0,0) origin at the top-left corner of the image. Later during user login, the system uses the originally recorded grid offsets to place the grid and determine the acceptance of the each login click-point.

During Password Creation:
Grid offset (Gx,Gy) used for grid positioning and can be calculated as,

$Gx = (x - r) \bmod 2r$

$Gy = (y - r) \bmod 2r$ where r is tolerance value

A Tolerence area identifier (Tx,Ty) is given by,

$Tx = (x - r)/2r$

$Ty = (y-r)/2r$

During Login:
First it retrieves the corresponding (Gx,Gy) for corresponding click point and calculate

$Tx = (x - Gx)/2r$

$Ty = (y-Gy)/2r$ and checks the current click-point falls in the grid or not.

For password generation SHA-1 algorithm is used. SHA1 is one way hash function. Password is generated using

PW=Hash([C1,.....,Ci],W,X]

where Ci=current click-point having [Ii,Gxi,Gyi,Txi,Tyi]

W= seed value.

X=User Name

5.3 View-Port Positioning Algorithm

The view-port positioning algorithm is used to encourage the user to select less guessable password. It helps the user to select the password but not impose the system generated password. Also the user has choice to select the number of click-point for password creation. Basically during password creation the part of an image which is less predictable is highlighted and user has to select the click-point within the highlighted portion and if the user is unable to select the click-point then he can move towards the next highlighted portion by pressing the shuffle button. The highlighted part of an image basically guides users to select more random passwords that are less likely to include hotspots. Therefore this works encouraging users to select more random, and difficult passwords to guess. During Login, images are displayed normally and user has to select the click-point as chosen at the time of password creation but this time highlighted portion is not present as it only provides the system suggestion.

6. Experimental Results

The result analysis of proposed system with existing technique is given by. Following figure 5 shows the result analysis when correct click-point is chosen during authentication or login time. For example during password creation if user has chosen (477,197) as a initial click point and if grid size is 19 X 19 than X axis Co-ordinate range from 468 to 486 and Y axis Co-ordinate range from 188 to 206. Now during login time if co-ordinates are (477,196) than it will check whether it lies within the 19 X 19 grid or not, based on that next image will be generated and from that user will know he is going wrong or right such that he recognizes the image during password creation and login are same or not. If user has chosen the correct click-point than he will get same image as that of creation time and he may proceed.

Click-point	Original Recorded (X,Y) Coordinates	Min and Max X-Coordinate Value for 19X19 Grid		Min and Max Y-Coordinate Value for 19X19 Grid		Login Time Recorded (X,Y) Co-ordinate	Accepted / Rejected
		Min X	Max X	Min Y	Max Y		
First	(477,197)	468	486	188	206	(477,196)	Accepted and Same Image will be shown
Second	(492,86)	483	501	77	95	(490,87)	Accepted and Same Image will be shown
Third	(127,192)	118	136	183	201	(126,192)	Accepted and Same Image will be shown

Figure 5. Result Analysis for Correct Click-point chosen

Licensed Under Creative Commons Attribution CC BY

Following fig shows the result analysis when incorrect click-point is chosen during authentication or login time. Now during login time if co-ordinates are (496, 97) than it will check whether it lies within the 19 X 19 grid or not, in below figure it is shown that the point lies outside the grid such as X lies within the x-axis whereas Y lies outside the y-axis so it is rejected by the system and different image will be shown. If he is the valid user than at any point he can start entry again where as attackers cannot recognize that he is going wrong.

Click-point	Original Recorded (X,Y) Coordinates	Min and Max X-Coordinate Value for 19X19 Grid		Min and Max Y-Coordinate Value for 19X19 Grid		Login Time Recorded (X,Y) Coordinate	Accepted / Rejected
		Min X	Max X	Min Y	Max Y		
First	(477,197)	468	486	188	206	(485,192)	Accepted and Same Image will be shown
Second	(492,86)	483	501	77	95	(496,97)	Rejected and Different Image will be shown

Figure 6. Result Analysis for Incorrect Click-point chosen.

7. Security Analysis of Graphical Password

7.1 Dictionary attack

In Graphical Password scheme dictionary attack is not possible because here user gives an input using mouse where as in case of text password user provides input through the keyboard which results dictionary attack is easily possible.

7.2 Guessing

The most basic guessing attack is Brute-force attack. Some Graphical Password system is vulnerable to guessing attack.

7.3 Shoulder Surfing

Like text password Graphical password is also vulnerable to Shoulder-Surfing attack.

7.4 Spy ware

Key logging or key listening spy ware cannot be used to break graphical passwords system. Mouse motion alone is not enough to break graphical passwords.

7.5 Social engineering

It is very difficult for a user to discuss regarding the graphical password as compare to text password. So Graphical Password Systems are free from Social Engineering attack

8. Conclusion

The major advantage of proposed scheme is that it provides larger password space then the alphanumeric passwords. For Graphical passwords there is a rising interest is that they are better than the Text based passwords, while the important argument for graphical passwords are that people are better at memorizing graphical passwords than text-based passwords. Also it removes the pattern formation and hotspot attack since it provides the system suggestion. Also the proposed system removes the shoulder surfing attack.

References

[1] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. van Oorschot, "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism," IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 2, March/April 2012.
[2] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The Memorability and Security of Passwords," Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, eds., ch. 7, pp. 129-142, O'Reilly Media, 2005.
[3] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2019 2020, Dec. 2003.
[4] A. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, June 2006.
[5] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray H*ill, NJ*, U. S. Patent, Ed. United States, 1996.
[6] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System," Int'l J. Human-Computer Studies, vol. 63, nos. 1/2, pp. 102-127, 2005.
[7] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," Proc. First Symp. Usable Privacy and Security (SOUPS), July 2005.
[8] A. Dirik, N. Menon, and J. Birget, "Modeling User Choice in the Passpoints Graphical Password Scheme,"

Licensed Under Creative Commons Attribution CC BY

Proc. Third ACM Symp. Usable Privacy and Security (SOUPS), July 2007.
[9] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.
[10] B. Fogg, Persuasive Technologies: Using Computers to Change What We Think and Do. Morgan Kaufmann Publishers, 2003.
[11] A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Improving Text Passwords through Persuasion," Proc. Fourth Symp. Usable Privacy and Security (SOUPS), July 2008.
[12] R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical Passwords:Learning from the First Twelve Years," to be published in ACM Computing Surveys, vol. 44, no. 4, 2012.
[13] S. Chiasson, J. Srinivasan, R. Biddle, and P.C. van Oorschot "Centered Discretization with Application to Graphical Passwords," Proc. USENIX Workshop Usability, Psychology, and Security (UPSEC), Apr. 2008.

Author Profile

Prof. Uma Yadav completed BE in Information Technology from Rashtrasant Tukdoji Maharaj Nagpur University, Nagpur in 2009 and M. Tech in Computer Science & Engineering from Rashtrasant Tukdoji Maharaj Nagpur University, Nagpur in 2013. She is currently the Assistant Professor in the department of Computer Science & Engineering in Shri. Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra, India.

Prof. Sarita Sakure completed BE in Computer Technology in year 2007 from Rashtrasant Tukdoji Maharaj Nagpur University, Nagpur, M. Tech in Computer Science & Engineering in year 2013 from Rashtrasant Tukdoji Maharaj Nagpur University, Nagpur and MBA in year 2015 from Rashtrasant Tukdoji Maharaj Nagpur University, Nagpur. She is currently the Assistant Professor in the department of Computer Science & Engineering in Dr. Babasaheb Ambedkar College of Engineering and Research, Nagpur, Maharashtra, India.

Licensed Under Creative Commons Attribution CC BY