International Journal of ChemTech Research
CODEN (USA): IJCRGG, ISSN: 0974-4290, ISSN(Online):2455-9555
Vol.10 No.14, pp 236-242, 2017

A study on graphical passwords

K .Keerthana*

Department of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Namakkal, Tamil Nadu, India

Abstract : Now a day's Communication, Reservation, shopping, Banking etc are done through authentication on corresponding websites. In this case secure authentication is very essential. About 97 % of people are using passwords for their authentication. Password is nothing but alphanumeric characters that provide access to particular websites or data. Setting a password which is simple, easy to implement and resist all types of attacks is highly challenging task. One way to face this challenge is using graphical passwords. In this paper we are going to analyze on different types of graphical passwords to get better protection from the prevailing attacks.

Keywords : Graphical Passwords, Captcha, Attacks.

Introduction

The idea of graphical passwords was first invented by Greg Blonder (1996). For Blonder, graphical password means it displays a predetermined sequence of images and user should select a predetermined region in every image to get access to particular assets. After that various graphical passwords have been invented. Password based authentication techniques are mainly categorized into three types. They are Biometric based authentication, Token based authentication and Knowledge based authentication. Biometric based authentication means identity of the individual is confirmed through his intrinsic characteristics. It includes retina, finger print etc. Token based authentication means identity of the individual is verified by the token provided by the server. Knowledge based authentication means identity of the individual is proven by his knowledge. For example, answering a secret question. Graphical password is one type of Knowledge based authentication.

Based on criteria graphical password is divided into two types. They are Recall based technique and Recognition based technique. In recognition based, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he selected during the registration stage. In recall based graphical password, a user is asked to reproduce something that he created or selected earlier during the registration stage[14].

Related Work

Securing password against online password guessing attacks using graphical password

It describes the system which uses Password Guessing Resistant Protocol. When user inputs one of the graphical password such as Pass Points (PP), Cued Click Points (CCP), Persuasive Cued Click- Points (PCCP), Audio Graphical Password (AGP) from client side to access assets using browser. It prevent the server from hacking[1]. The server must usesPassword Guessing Resistant Protocol to identify the legitimate users to avoid unauthorized access.

Revisiting defenses against large-scale online password guessing attacks

This paperbriefly describes about the Password Guessing Resistant Protocol [PGRP].PGRP has both graphical user interfaces (browser-based logins) and character-based interfaces (SSH logins). It enforces ATTs after a few (e.g., three) failed login attempts from unknown machines[2]. It identifies the machines through cookies and IP address of the system. Cookies are the input for PGRP algorithm for granting access for the system. The author also compares security of PGRP in single and multiple attacks with other ATT based protocols such as Pinkas and Sander, van Oorschot and Stubblebine. Finally the author concludes that PGRP is significantly better in security and usability when compared to other ATT based protocols[3].

Password guessing resistant protocol

It explains how PGRP evolved from Automated Turing test ATTs. It explains the working of PGRP when an individual try to access from a known or unknown system. It also describes about its three data structure namely whist list, blacklist and failed login from valid IP. Features such as inaccessible sites and multiple ATTs are added to PGRP to enhance the security of PGRP. In this system username and password of an individual is given as input for PGRP and after verification it declares the individual as legitimate user or an unlawful user.

Graphical password authentication using persuasive cued click point

This paper depicts a detailed view about the various method of recall based technique. It elucidate the concept of PassPoints (PP), Cued Click-Points (CCP).It improve Cued Click-Points by adding Persuasive technology to it to obtain Persuasive Cued Click-Points (PCCP).PCCP allow us to tap on every image but within view port or tolerance region which avoid the creation of new hotspot and discovering the known hotspot became harder. PCCP contains two modules namely User registration module and Login module. Each modules flow chart is explained in this paper. Based on the tolerance value [degree of closeness to actual click] the security rate of PCCP varies. This system analyzes the various factors of PCCP and CCP such as login and security success rates, speed, time and produce result as PCCP is efficient in security than CCP.

Defending online password hunch attacks using persuasive cued click points

This paper has implemented the authentication system based on three modules namely PassPoints (PP), Cued Click-Points (CCP) and Persuasive Cued Click-Points (PCCP). The requirement of the system is analyzed through Software Development Life Cycle [SDLC] and the system is developed using SPIRAL model. The system uses ASP .Net and C#.net technology. Since the project is a click based system, the input is given as click points and the system validate the clicks and allow or deny the user to access the system. It also performs test cases on each and every module present in the system.

CARP: Captcha as a graphical password based authentication scheme efending online password

It explains every technique of graphical passwords. It includes passfaces, Déjà vu scheme and Story Scheme in Recognition based technique, Draw–A-Secret (DAS) Scheme in Recall based technique and Blonder technique and PP in Cued Recall Based Technique. To overcome the drawbacks of all these techniques CAPTCHA has been invented and it is used as graphical password known as CaRP [Captcha as a graphical Password]. CaRP can be categorized into Recognition based and Recognition-Recall. In this system security is implemented at two modules one will be captcha authentication and the other will be at opening or downloading a file [optional]. During captcha authentication a set of images will be displayed and user must select correct graphical captcha and while securing document an image is displayed and user should select correct PassPoints to access the document. Here graphical captcha and passpoints are given as input to find the legitimate user.

A novel graphical password authentication mechanism

The author proposes a new method for setting a strong password. This system has five steps to set a strong password. First, the user must select an image then the portion of that image is selected as password. Second, the user is provided with the rolling numbers either user can insert any random numbers or press start button which will displays the random numbers. While login the user should select image that contain predetermined random numbers. After the successful completion of two phases the user is asked to enter their username and password. Finally, the user is asked to enter the captcha which is generated by the system. In this system click points, image of rolling numbers, password and captcha is given as input which will strongly resist all type of attacks.

Implementation of graphical passwords using random codes

In this paper, the authorsays about the system that uses the random code which is hidden inside the image is used as password for authentication. To execute this process Least Significant Bit (LSB) algorithm is used to hide the code into the image. Here an image and random code are given as input for LSB which produce the output as an image. While login phase the individual must select correct image that contain predetermined random code. Then the code is extracted from that image and it is compared against code stored in database. After this verification the individual is allowed to access the assets. To enhance the security individual's email id is also verified.

A security class project in graphical passwords

This project uses a new method instead of graphical passwords. The dilemma of the graphical passwords is that such system may require an inordinate amount of storage space for images. To eliminate the need for high disk space by using an online picture database and calling an external server each time the user clicks. To avoid this, our system is based on the user interface of zooming into Google maps which avoids the calling an external server. Users are familiar with zooming into a specific area of interest, such as a street location. By overlaying a 2D grid on the map and user can select levels for zooming into the grid to navigate to a specific location. This location can use as password and it is equivalent to selecting a sequence of images in the CCP technique.

GRAMAP: three stage graphical password authentication scheme

This paper says the user can select the levels of security. At first level user should select the continent and need to click on one of the gateway points located on that continent finally the user should select the country present inside the continent. Now there is only one gateway point on each state. Clicking of a gateway point completes first level. Only the values of gateway points are saved as password. In second level the user should select an image from set of images. During authentication the same image will be displayed only when the values of gateway points are same. The third level of security is also optional where the user should decide the number of clicks in that image. For accurate clicks here hint icons are provided. User should click the predetermined hint icons to use or access the system.

Analysis

This section presents the comparisons on Existing graphical password techniques. This study helps us to find the drawbackspresent it in the existing system. Based on this analysis, the proposed system will be designed.

Table 1.Input and Output of Graphical Password Techniques

SI.No	Name of The Technique	Input	Authentication Process	Output
1.	Blonder	User click on the tap region of image	Verify the user click is same as the predetermined click of user done in registration process	If yes, then User can access the system or data If no, access denied
2.	Draw-a-Secret [DAS]	User Draw something on 2D grid[7]	Ensuring redrawn lines are in exact position by validating the coordinate values stored in database.	If yes, then User can access the system or data If no, access denied

3.	PassFaces	User will identify and select the predetermined face image for several rounds[15]	Verify the face image is identical as predetermined in registration process	If yes, then User can access the system or data If no, access denied
4.	Dejavu	User select a certain number of random art pictures	Verify the obtained seed value with the database	If yes, then User can log on the system .If no, access denied
5.	Story Based Passwords	User Select the images based on story remembered by them	Validate the sequence of selected image with the sequence stored in server	If yes, then User can access the asserts on the system. If no, access denied
6.	PassPoints [PP]	Click locations of a picture within the tolerance region in right sequence	Verifying the click points selected are in same order as in Registration phase	If yes, then User can log on the system. If no, access denied
7.	Cued Click Points [CCP]	User make single click on multiple sequence of images	Verify the click points are within the tolerance region[13]	If yes, then User can log on the system. If no, access denied
8.	Persuasive Cued Click Points [PCCP]	user click one point per image for a sequence of images	Verify the click points are within the tolerance region	If yes, then User can log on the system[5]. If no, access denied
9.	Captcha	User should type the random characters displayed by server or click the image based on constrains	Verify the characters entered Or image selected by the user are correct	If yes, then User can log on the system. If no, access denied
10.	Google Maps	User Select a location on a map	Validate the obtained coordinate values with the values stored in database	If yes, then User can log on the system If no, access denied

Table 2.Merits and demerits of Graphical Password Techniques

SI.No	Name of the Technique	Resistable Attacks	Non Resistable Attacks	Advantage	Disadvantage
1.	Blonder	Dictionary Attack	Shoulder Surfing and Spyware attack	Easier to recall and provide higher security than alphanumeric passwords	Number of predefined regions is small which leads to lower security
2.	Draw-a-Secret [DAS]	Spyware attack	Shoulder Surfing and Dictionary Attack	Language independent and Users are liberated from remembering any alphanumeric string.	Redrawing in exact position is difficult[11]

3.	PassFaces	Tricking	Shoulder Surfing and Dictionary Attack	Easy to remember	Probability of a guessing attack is high
4.	Dejavu	Dictionary Attack and Tricking	Shoulder Surfing attack[8]	Convenient to store and transmit the art images	It is difficult to record, share or remember the art image and the password space is much smaller than alphanumeric passwords
5.	Story Based Passwords	Dictionary Attack	Shoulder Surfing	Only one round of authentication is needed	User find Hard to remember the story
6.	PassPoint [PP]	Tricking	Dictionary Attack and Phishing	This method overcome the drawback of blonder by enabling the user to click as many points as possible in the image which increase the security level	Time consuming and difficult to memorize the click points
7.	Cued Click Points [CCP]	Tricking, Phishing	Dictionary Attack and shoulder surfing attack	Larger password space	Passwords can be guessed through Hotspots[4]and the process is time consuming
8.	Persuasive Cued Click Points [PCCP]	Hotspots, Tricking, Phishing and Dictionary Attack	Spyware attack and shoulder surfing attack[12]	Reduces hotspots and pattern formation	Passwords can be broken when input sequence or login process is captured by hackers
9.	Captcha	Dictionary Attack, Shoulder Surfing, Tricking, Phishing and Spyware attack	Non legitimate user access	Users are liberated from remembering the passwords[6] and it resist bots from accessing the data.	Unable to recognize the unauthorized personnel authentication
10.	Google Maps	Shoulder surfing[10]	mouse loggers	Easy to remember the locations	Requires High disk space[9]

Result and Discussion

After analyzing each password technique the possible steps to overcome the prevailing attacks are given below:

Step-1 Initially Check the website is original or phishing website before entering a password.
Step-2 Users must enter the captcha generated by the server to verify that whether a human is accessing that website. This process prevents the bots from accessing the website.

Step-3 Enter the username or user id of an individual
Step-4 To verify that respective individual is accessing the website check the intrinsic characteristic [except fingerprint because it is easily traceable]
Step-5 After the verification of intrinsic character of a user a one time password is sent to the user's mail id which has been entered by the user during registration process
Step-6 The user should enter the opt for the session
Step-7 Finally users are asked to enter the passwords to access the data. And users are allowed to enter only the image passwords because the image passwords are more securable than text passwords

But the user can embed a Random unique code or text inside a picture and using that picture as a password will resist from brute force attack, dictionary attack, shoulder surfing attack etc.

Conclusion

In Summary, we proposed a survey on graphical passwords and we compared various graphical password schemes by analyzing the resistance [able to tolerate the attack] and non resistance of each graphical password. Based on this analysis we came to know the drawbacks of each graphical password. By examining the reasons which make the password vulnerable & insecure we have proposed possible steps. In future we going to take steps to implement the solution what we have proposed which give better security than the existing password techniques.

References

1. Poonam M. Khairnar, Kirti K.Nagare, RitikaV.Agrawal and Ashwini U. Mahale. Securing Password Against Online Password Guessing Attacks Using Graphical Password. Imperial Journal of Interdisciplinary Research (IJIR). Vol-2, Issue-3, 2016,ISSN : 2454-1362.
2. MansourAlsaleh, Mohammad Mannan, and P.C. van Oorschot. Revisiting Defenses Against Large-Scale Online Password Guessing Attacks. IEEE Transactions On Dependable And Secure Computing.Vol. 9, No. 1, Jan/Feb 2012.
3. Arya Kumar,A. K. Gupta.Password Guessing Resistant Protocol.International Journal of Engineering Research and Application. ISSN : 2248-9622, Vol. 4, Issue 2(Version 1), February 2014, pp.656-660.
4. Iranna A M,Pankaja. Graphical Password Authentication Using Persuasive Cued Click Point.International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering.ISSN (Print): 2320 – 3765, ISSN (Online): 2278 – 8875, Vol. 2, Issue 7, July 2013.
5. D.Lavanya, Bethini Saiteja, S. Bala Moulika and P.Rakesh Reddy. Defending Online Password Hunch Attacks Using Persuasive Cued Click Points. International Journal Of Engineering Sciences & Research Technology. 2014, ISSN: 2277-9655.
6. Shraddha S. Banne, Kishor N. Shedge. Carp: Captcha As A Graphical Password Based Authentication Scheme.International Journal of Advanced Research in Computer and Communication Engineering.Vol. 5, Issue 1, January 2016 ISSN (Online) 2278-1021 ISSN (Print) 2319 5940.
7. Delphin Raj K M, Nancy Victor. A Novel Graphical Password Authentication Mechanism.International Journal of Advanced Research in Computer Science and Software Engineering.Volume 4, Issue 9, September 2014 ISSN: 2277 128X.
8. D.S.Gawande, Manisha P. Thote, Madhavi M. Jangam, Payal P. Khonde, Payal R. Katre, and Rohini V. Tiwade. Implementation of Graphical Passwords Using Random Codes.International Journal of Computer Science and Mobile Computing.2320–088X, Vol. 5, Issue- 3, March 2016, pg.517 – 524.
9. Jake Spitzer, Cal Singh, Dino Schweitzer. A Security Class Project in Graphical Passwords.
10. S.Rajarajan, M. Prabhu, S. Palanivel andM.P.Karthikeyan.Gramap: Three Stage Graphical Password Authentication Scheme.Journal of Theoretical and Applied Information Technology.20th March 2014, Vol. 61 No.2, ISSN: 1992-8645 E-ISSN: 1817-3195.
11. MokalPranitaHaridas, R. N. Devikar.A Comparative Study of Graphical Passwords And Their Security Issues. International Journal of Advanced Research in Computer Science and Software Engineering.Volume 5, Issue 7, July 2015 ISSN: 2277 128X.
12. Arti Bhanushali, Bhavika Mange, HarshikaVyas, Hetal Bhanushali and Poonam Bhogle.Comparison of Graphical Password Authentication Techniques.International Journal of Computer Applications.Volume 116 – No. 1, April 2015.

13. Haichang Gao, Wei Jia, Fei Ye and Licheng Ma.A Survey on the Use of Graphical Passwords in Security.Journal of Software.Vol. 8, NO. 7, July 2013.
14. D.Aarthi, Dr.K.Elangovan. A Survey on Recall-Based Graphical User Authentications Algorithms.International Journal of Computer Science and Mobile Applications.Vol.2 Issue. 2, February- 2014, pg. 89-99, ISSN: 2321-8363.
15. XiaoyuanSuo.A Design and Analysis of Graphical Password. Georgia State University,2006.

*****