ISSN:0975-9646

To Mitigate Online Password Guessing Attack By Implementing: P3-HA

P.P Wakodikar , A.S. Bhattacharya

[1]*Department of Computer Science and Engineering,*
GHRIETW, 440016, Nagpur,
MH, INDIA

Abstract: **Most preventive and safe passwords are pictorial based password as compared to dextral based, password as far as authentication is concerned. This research is based on the human need regarding with their privacy and usefulness. Privacy deals with preventing user information from anti-social activity and usefulness in terms of the human power of remembrance. By putting such concept this paper proposes a new algorithm called as P3-HA (Pictorial PanOut Password - Hunch Attack) which is an advance version of previous pictorial techniques. The proposed system instead of dextral based passwords uses pictorial based password. P3-HA limits total number of click event generated in an image during selecting the password. It not only restrict failed attempt on dextral during login but also it restricts the number of trial attempts after the image challenge is given.**

Keywords: Dextral based password, Hunch attack, Pictorial based password.

INTRODUCTION:

For prevention of user account passwords are generally used. But, the passwords have various drawbacks related to their security and strength. Hence, researchers focus deals with the preventive measures for making passwords more secure and powerful. Pictorial based password is one of the strongest ways to prevent password from unwanted entry to break or crack password. Instead of dextral based now-a-days pictorial passwords is generally used due to various drawbacks of the dextral based system and various advantages of pictorial based system. In terms of user usability and security pictorial password are very much beneficial. Lots of researchers deal with such type of passwords, but there is no satisfactory measure comes forward. P3-HA abbreviated for Pictorial PanOut Password- Hunch Attack is a new technology which deals with not only security but also with the usability of the user by improving user tendency to remember password and hard to identify password to an attacker. This system uses dextral-pictorial password which makes the system stronger than any other techniques. The basic difficulty comes forward is shoulder surfing attack. P3-HA is very much helpful to mitigate such type of attack. In this system user provide with a not only dextral password, but also pictorial password. If user remembered his password he can directly access his account. But if he forgot his password, then he will access his account with the help of pictorial password. So this system maintains usability. As far as security is concerned P3-HA restricts the number of wrong attempts not only in dextral based but also in pictorial based. Also, each time during login a user will get scrambled image therefore it is hard to guess the image for the dirty deed. Hence P3-HA is a very effective approach as compared to previous approaches.

A. A. Related work:

Various researchers show that as compared to the dextral based user will like to use pictorial password for their privacy issues. As passwords are very famous means used for endorsement and there are so many works done by various researchers regarding password security, as various kinds of attacks get performed on passwords like online and offline attacks. In online attack, brute force and dictionary based attacks are widely spread. Whereas shoulder surfing attack is also become very much serious problem with guessing the password. And to reduce such type of attack many researchers find various solutions with some satisfactory result and some are not. From all these types of attack guessing attack is very hard to detect. Passwords are categories into two types as dextral based and pictorial based. In [1] to prevent guessing attacks give number of trails to stop hacking. Old techniques which were very much used previously is locking technique, which lock certain accounts after the trails exceed threshold value [3]. But this is not a satisfactory solution for a legitimate user as some time user may mis-type or forget his password [8]. This type of attempt can also reduce by using a simple 3-key exchange protocol [7] or key junction protocol in which password is shared between two parties. By this, several text based techniques, many authors comes to know the usability problem. Usability is very much important as far as user satisfaction is concerned.

Graphical or pictorial based system solves the usability problem. Human tendency of grasping image is better than any text based system. The very first technique comes forward was CAPTCHA technique. This technique is very simple to identify the human generated password of server generated password [2]. [4] Categorized pictorial password in two ways- Recognition based or Recall based. In such type of system, the user generates a sequence in image or identify the previously selected image. In both techniques the usability gets affected and it is a very time consuming process. Passfaces is a very useful technique in terms of usability, but require a very large database to store various images. So from this review it comes to know that there is no satisfactory result yet to be found which reduces such type of hunch attacks.

B. ***Our Contribution:***

As we have seen from various studies that there is a large requirement of security and usability in any endorsement techniques. So, this paper contributes new technique called P3-HA that is Pictorial PanOut Password- Hunch Attack which combine dextral and pictorial based password together to prevent security and usability constraint. Using image user can remember it very easily, hence usability get maintain and the sequence of random image is very hard to guess so it is more secure to use image as a password. And using both types of password security issue also gets solved. In this proposed technique attacker have to face challenges in two ways. One is CAPTCHA and another one is shuffled image. The complete technique is explained in the next section.

C.. Organization

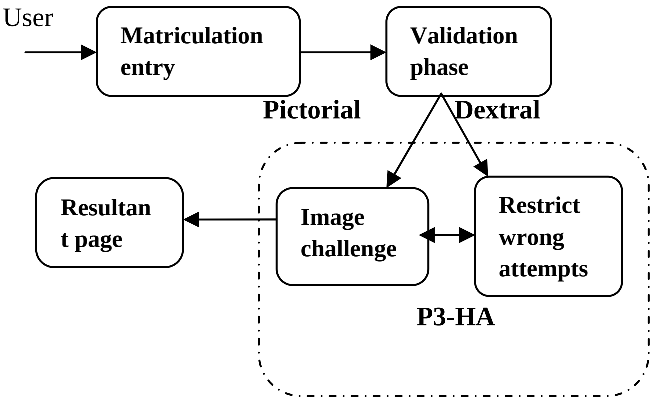
In section 2 we discuss proposed technique P3-HA with its functional module, and algorithm. Various module descriptions with their databases used discuss in section 3. In Section 4, we describe the application of the proposed system over previous approaches followed by their comparative result analysis in section 5. Section 6 draws a concluding remark.

II. PROPOSED MODEL: P3-HA (PICTORIAL PANOUT PASSWORD- HUNCH ATTACK)

The new concept called P3-HA uses dextral based and pictorial based as a password. It challenges attacker by CAPTCHA to identify the user information is the human generated or server generated and another is an image challenge in which user have to select the correct sequence as a click points to get authenticated.

This image was given to the user at the time of registration. So, only authorized user know about the sequence used in an image. The image is divided into 16 grid cell and user have to click on 5 cells to generate his secret. Hence our proposed system is very much preventive and secure as compared to other image based techniques. Again at the time of challenge attacker will get scrambled image and he has to identify the correct sequence to get access. The number of click points is restricted with 3 attempts only after that the user gets blocked. This complete scenario is explained in the algorithm describe further.

A. ***Functional diagram of P3-HA***



Functional diagram consists of an authorized user with his matriculation entry which then pass in validation phase to check whether the entry is by valid user or not by two ways. First for the wrong entry it first checks with the dextral based and restrict wrong attempts by 6 after that it check it by pictorial based after crossing the threshold value. If for same user name the entry was correct, then he first have to pass a dextral challenge after that image challenge. If selection <3 then he will get access else user get blocked. This two approaches together makes our system P3-HA.

B. Algorithm:

Necessary requirements-

Define

UT- user testimony
Ticket- user password
Snap – selected position
Ky1=6 - Ky2=3 - keys
Ip- source IP
TL- true list
FA- False Attempt
FT- Fake trial

To grant access for valid user and password Check

Valid IP, UT, Ticket or Ticket< Ky1
Put 0 value in FA and IP into TL
Display “Access granted”

For wrong user testimony

For invalid IP, UT put 1 value in FA
Provide CAPTCHA challenge. If challenge passed then enter into login page.
Else display “rejected”.

For wrong Ticket

Increase the value in FA until FA= Ky2. Else put value 1 in FT until FT=Ky2.
If total wrong attempt= Ky1, challenge user with CAPTCHA. If passed enter into login page.
If valid UT and Ticket, challenge it with image else go to step 8.
If correct Snap= 5 go to step 3, else for wrong selection Snap=3 user blocked.

III. MODULE DESCRIPTION:

A. A valid user data: In this module if user testimony and tickets valid then user don’t have to pass any challenge. He has authority to direct get access to his account.

B. Wrong user testimony: If user testimony is wrong the system considered it as a new user and challenge it with CAPTCHA technique. After passing the test it shows the login page. If the user is new user then he directly goes to the registration page, filled his necessary filled and then use login page or, if he is attacker then he try to crack the user testimony, but unable to break it as there is no way to guess user testimony.

C.Wrong user ticket: user will get valid 3 attempts to identify his password, if not, then he again gets 3 fake attempts to guess his password if he is a valid user. Then user challenged with CAPTCHA after exceeding 6 attempts if he passed the challenge the he will directly get an image which was selected at the time of registration. So, only valid user can identify the correct sequence of image.

But if the guesser was an attacker then he will have less number to identify the ticket or if he guessed the ticket than also he have to first pass the CATCHA challenge and then image challenge. It is very hard for attacker to guess. As that image was scrambled image and for identification of click points he only gets 3 wrong attempts to identify the click points. Else the user will get blocked.

After the correct login user can check his account and verify that how many times someone tries to break his code by the three databases as true list, false attempts and fake trails.

D.*Database:*

In our proposed system three databases are maintained to check how many times the particular account was in danger.

i. ***True List:*** This table stores the valid user testimony with his valid ticket with their IP address from which the valid login takes place with login date.

ii. ***False Attempts***: This table stores total number of valid login and 3 basic wrong attempts if any with IP address and Login count.

iii. ***Fake Attempts***: This table shows the remaining 3 trails that are fake attempts, from which user identify that their attack made by third party. This entry made when the opponent exceeds false attempts. This table have the user name to login count.

APPLICATIONS

As far as both types of password is concern P3-HA provide more secure and user friendly environment. Due to restrictive in nature P3-HA prevents online guessing attack as brute force and dictionary based attack. Also, due to the scrambled nature of image visitor from back side could not get recognize the exact position of click point which reduces shoulder surfing attack. Also, using one image for one user reduces data storage or disk space and also require less time to get authenticated. User satisfies in both ways in terms of usability and security. Overall performance of P3-HA is satisfactory in all cases as compared to previous approaches.

V. RESULT ANALYSIS:

A.Security Analysis:

↓ Reduce	PGRP	PASSPOINT	P3-HA
Brute Force Attack	✓	X	✓
Dictionary Attack	✓	X	✓
Shoulder Surfing Attack	X	✓	✓

From the above security analysis, it comes to know that P3-HA reduce all three types of attacks. From the table it shows that PGRP is very much effective to prevent the system from brute force and dictionary attack. Whereas passpoint technique reduces shoulder surfing attacks.

B. Usability Analysis:

	PGRP	PASSPOINT	P3-HA
Restrict no. Of attempts	✓	X	✓
Provide captcha challenge	✓	X	✓
Provide image challenge	X	✓	✓

As far as usability is concerned PGRP and P3-HA restrict the number of wrong attempts and provide CAPTCHA as a challenge. Whereas this technique is not with passpoint technique. As far as image is concerned P3-HA and passpoint technique used it and prevent it to get attacked by an attacker. From these scenarios also P3-HA is better in all means of usability.

V. CONCLUSION :

This paper makes two kinds of contribution. First relate to security constraint and another is password persistent. From the related research, it comes to know that there are various addresses available to make user password more secure and memorable, but there is no proper solution to mitigate different types of attacks over passwords. Since to make password stronger and harder to guess pictorial password is the best solution which makes user convenient to select password of user own choice. In contrast P3-HA is more restrictive than any other technique in terms of both dextral based and pictorial based password. Up till now no such system develops which reduces shoulder surfing attack, brute force attack and dictionary based attack. It provides more security to the user and prevents users from anti-social activity.

REFERENCES:

[1] Steven M. Bellovin, Michael Merritt "Encrypted Key Exchange: Password Based Protocol Secure Against Dictionary Attacks ", Symposium on research in security and privacy (RISP), IEEE 1992. http://dx.doi.org/10.1109/risp.1992.213269

[2] Monica Chew and J.D Tygar, UC Berkely, " Image Recognition CAPTCHA", 7th international Information Security Conference, Springer 2004. http://dx.doi.org/10.1007/978-3-540-30144-8_23

[3] Susan Wiedenbeck Jim Waters, Jean- Camillee Bringer Alex Brodskiy, Nasir Memon " Authentication using Graphical Password Effect of Tolerance and Image Choice", Symposium on Usable Privacy and Security, 2005. http://dx.doi.org/10.1145/1073001.1073002

[4] Mohammed Misbahuddin, Dr P. Premchand, Dr A. Govardhan "A User Friendly Password authenticated Key Agreement for Web based service", International Conference on Innovations in Information Technology, (ICIIT) IEEE 2008. http://dx.doi.org/10.1109/innovations.2008.4781766

[5] Alireza Pirayesh Sabzevar, Angelos Stavrou, "Universal Multi-Factor Authentication Using Graphical Passwords", International Conference on Signal Image Technology and Internet Based Systems (ICSITAIBS) IEEE 2008 http://dx.doi.org/10.1109/SITIS.2008.92

[6] Amirali Salehi-Abari, Julie Thorpe, and P.C. van Oorschot, “On Purely Automated Attacks and Click-Based Graphical Passwords” Annual Computer Security Applications Conference (ACSAC)2008 http://dx.doi.org/10.1109/ACSAC.2008.18

[7] Haichang Gao, Xiyang Liu, Ruyi Dai, Sidong Wang, and Xiuling Chang, “Analysis and Evaluation of the ColorLogin Graphical Password Scheme”, 5th International Conference on Image and Graphics (ICIG) 2009. http://dx.doi.org/10.1109/icig.2009.62

[8] M. Martinez-Diaz, C. Martin-Diaz, J. Galbally and J. Fierrez, “A Comparative Evaluation of Finger-Drawn Graphical Password Verification Methods”,12th International Conference on Frontiers in Handwriting Recognition (ICFHR) 2010. http://dx.doi.org/10.1109/icfhr.2010.65

[9] Daniel LeBlanc, Alain Forget and Robert Biddle, “Guessing Click-Based Graphical Passwords by Eye Tracking”, 8TH Annual International Conference on Privacy, Security and Trust(PST) 2010 http://dx.doi.org/PST.2010.5593249

[10] Wei Hu,Xiaoping Wu, Guoheng Wei “The Security Analysis of Graphical Passwords”, International Conference on Communications and Intelligence Information Security (ICCIIS) 2010 http://dx.doi.org/10.1109/ICCIIS.2010.35

[11] M.Arun Prakash, T.R.Gokul, “Network Security-Overcome Password Hacking Through Graphical Password Authentication” Proceedings of the National Conference on Innovations in Emerging Technology, (NCIET)2011. http://dx.doi.org/10.1109/NCOIET.2011.5738831

[12] Kuo-Feng Hwang, Cian-Cih Huang, Geeng-Neng You, “A Spelling Based CAPTCHA System By Using Click” International Symposium on Biometrics and Security Technologies (ISBAST) IEEE 2012. http://dx.doi.org/10.1109/ISBAST.2012.17

[13] Joseph Bonneau, “The science of guessing: analyzing an anonymized corpus of 70 million passwords” Symposium on Security and Privacy (SSP) IEEE 2012 http://dx.doi.org/10.1109/SP.2012.49

[14] Hani Moaiteq Aljahdali, Ron Poet, “The affect of familiarity on the Usability of Recognition-based graphical Password” 12th International Conference on Trust, Security and Privacy in Computing and Communications (ICTSPCC) IEEE 2013 http://dx.doi.org/10.1109/TrustCom.2013.187

[15] Anthony Vance, David Eargle, Kirk Ouimet, Detmar Straub, “Enhancing Password Security through Interactive Fear Appeals: A Web-based Field Experiment” 46th Hawaii International Conference on System Sciences (HICSS) IEEE 2013 http://dx.doi.org/10.1109/HICSS.2013.196

[16] Akihiro Satoh, Yutaka Nakamura, Takeshi Ikenaga, “Identifying User Authentication Methods on Connections for SSH Dictionary Attack Detection” 37th Annual Computer Software and Applications Conference Workshops (CSACW) IEEE 2013 http://dx.doi.org/10.1109/COMPSACW.2013.80

[17] Hector Marco-Gisbert, Ismael Ripoll, “Preventing brute force attacks against stack canary protection on networking servers” 12th International Symposium on Network Computing and Applications (ISNCA) IEEE 2013. http://dx.doi.org/10.1109/NCA.2013.12

[18] Keisuke Kato, Vitaly Klyuev, “Strong Passwords: Practical Issues” 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) IEEE 2013 ttp://dx.doi.org/10.1109/IDAACS.203.6662997