International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 12, December-2015

A survey on Graphical Password Authentication

Shiksha Saxena
Mtech C.S.E.,LNCTS Bhopal
LNCTS Bhopal
Bhopal, India

Nikesh Tiwari
Assistant Professor C.S.E. LNCTS Bhopal,
LNCTS Bhopal
Bhopal, India,

Abstract: **The most common authentication technique is to use alphabetical usernames and passwords. This system has been shown to possess necessary drawbacks. As Associate in nursing example, users tend to pick passwords that will be merely guessed. On the other hand, if a word is troublesome to guess, then it's always arduous to remember. to deal with this disadvantage we've a selection sort of a graphical positive identification. That is associate authentication system that works by having the user select from photos, throughout a selected order, given throughout a graphical worm (GUI).**

I. INTRODUCTION

In recent years, information security has been developed as a very important drawback. Main space of knowledge security is authentication that is that the determination of whether or not a user ought to be allowed access to a given system or resource. During this context, the positive identification could be a common and wide authentication methodology. A positive Identification could be a kind of secret authentication that's wont to management access to knowledge. it's unbroken secret from unauthorized users, and people want to realize access square measure tested and square measure granted or denied the access supported the positive identification according to that Passwords square measure used from ancient times itself as the distinctive code to discover the malicious users[1].

In trendy times, passwords square measure won't to limit access to guard laptop operational systems, mobile phones, and others. Somebody may need passwords for several uses like log in to private accounts, accessing e-mail from servers, retrieving files, databases, networks, web sites, etc.

Normal watchwords have some drawbacks such as hacked password, forgetting watchword and purloined watchword thus, sturdy authentication is required to secure all our applications. standard passwords have been used for authentication however they square measure familiar to have issues in usability and security. Recent days, another technique such as graphical authentications introduced. Graphical watchword has been planned as associate different to alphanumerical watchword. Psychological studies have shown that individuals will keep in mind pictures higher than text. Pictures square measure typically easier to be remembered than alphabets and numbers, particularly photos, that square measure even easier to be remembered than random image .[2]

II. LITRATURE RIVEW

In this section a literature review for the ways that represent the graphical secret authentication theme

Rosa Lin, Shih-Yu Huang [3] presents a CAPTCHA design technique which specially designs for mobile users. In that technique a new CAPTCHA designing interface called CAPTCHA Zoo is presented that utilizes human vision property to design CAPTCHA. That uses the property of human vision system which is able to recognize shapes from naturally colored and arranged backgrounds. That uses parameterized 2D projection of 3D models to design CAPTCHA. That provides an efficient CAPTCHA designing technique even in the case of varying parameters.

Bin B. Zhu, Jeff Yan, Qiujie Li [4] presents, an image recognition CAPTCHA called cortcha which provide solutions for large scale applications. Cortcha based on the recognizing objects on the basis of its surrounding context, a task that human can perform better than computer. In that paper analysis over different attacks is performed and then on the basis of that analysis cortcha is designed and in that design machine learning process is avoided that put significant improvement to reduce the attacks related to machine learning algorithms.

Niket Kumar Choudhary, Rahul Patil[5] a three CPATCHA based design called BarCAPTCHA, TransparentCAPTCHA, ThreadCAPTCHA is presented. That CAPTCHA design is based on the principle of hard to separate background". In BarCAPTCHA small bars are used to show text and create noise in the background. In transparent CAPTCHA, text is written in the form of transparent font on image. In thread CAPTCHA text is written in the form of looks-like long thread. Hus this provides enhanced security mechanism and hard to break too.

Shubhangi G. Hande, M.S. Ali [6] presents CAPTCHA which is mirrored and reversed and provide user to identify that CAPTCHA thus made it secure and robust to attacks. In that technique if user enters wrong CAPTCHA then a message is shown called login failed, if user enters correct CAPTCHA then user redirect to the user page.

R.Biddle, S. Chiasson [7] presents three type of graphical password. Recognition based Graphical password, cued recall graphical password, and recall based graphical password. In recall based graphical password user need to recall password without any cue, in recognition based graphical password user need to recognize password from the set of image, in cued recall graphical password some cue is provided to identify password from the image.

H.Tao, C. Adams [8] presents a grid based CAPTCHA password called Pass Go. In that CAPTCHA user need to select meeting point of the grid. That password based on a Chinese game called Pass Go which is based on simple rule and very famous among the users. It also uses draw a secret to enhance the security of the system.

Ian jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin, USENIX Security Symposium [9] Outline of graphical secret key adventures the components of graphical data presentations to accomplish preferable security over content based passwords. Graphical information gadgets empower the client to decouple the position of inputs from the fleeting request in which those inputs happen, and we demonstrate this decoupling can be utilized to create secret word plans with considerably bigger (essential) watchword spaces. With a specific end goal to assess the security, a novel way is formulated to catch a subset of the huge passwords that is the configuration of graphical passwords. This is fundamentally inspired by gadgets, for example, individual computerized colleagues (PDAs) that graphical info capacity through a stylus or a mouse.

III. SECURITY ATTACKES IN GRAPHICAL PASSWORD AUTHENTICATION

There are few attacks in Graphical Password Authentication:

1. *Shoulder surfing attacks:*

Shoulder water sport attack refers to attack the user passwords by victimization direct observation techniques. Main direct observation technique is trying over someone's shoulder to urge the countersign. Shoulder water sport attack largely happens publically places as a result of its very easy in an exceedingly crowd to face close to somebody and appearance at them coming into a countersign or any secret key.

2. *Guessing attacks*

Many users tend to pick out their passwords supported their personal info just like the name of their pets, house name, phone range, passport range, etc. In these cases, the assailant tries to guess the parole by making an attempt the main parole prospects based mostly on the user's personal info. Dead reckoning attacks will be generally classified into two categories: on-line parole dead reckoning attacks and offline parole dead reckoning attacks. In on-line parole dead reckoning attack, assailant tries to guess a parole by manipulating the inputs of one or additional oracles. In offline parole dead reckoning attack, assailant thoroughly searches for the parole by manipulating the inputs of 1 or additional oracles

3. *Spyware Attack*

Spyware is a sort of malicious software package that put in on computers with the aim of stealing secret info of users. Spyware attack is ordinarily done by victimization a key feller or key observer. This malwares gathers info while not user's information concerning gathering and leak this info to an outdoor supply of wrongdoer

4. *Social engineering attack:*

Social engineering is the attack, in that human gains the sensitive info from the human interaction. In this sort of attack, aggressor tries to get the knowledge regarding a company or pc systems from the user itself to act like associate worker. The aggressor doesn't use any electronic techniques of hacking during this quite attack as he or she uses solely human intelligence and tough voice communication to get the info he desires. Once aggressor gets some of data from one supply, then he or she might gather info from alternative sources among identical organization to induce the entire info and increase his or her quality.

5. *Dictionary Attack*

In this attack, AN offender tries to guess the parole from a awfully massive list of words, dictionary. Lexicon is the assortment of all high likelihood passwords supported previous alternatives. If a user chooses a parole, a word already inside the lexicon, then this attack can be flourishing. This attack is a specific kind of the parole brute forcing attack. [10]

IV. CONCLUSION

CAPTCHA (Completely Automatic Public Turing Test to Tell Computers and Humans Apart), are the graphical passwords which are used to generate test that only human can solve. In many online applications CAPTCHAs are used to protect from various attacks. In this paper a survey over the different technique is presented which are used to design CAPTCHA. For future work, an enhanced CAPTCHA framework is design to provide security from various attacks like brute force attack, denial of service attacks etc

REFERENCES

[1] Phen-Lan Lin, Li-Tung Weng and Po-Whei Huang, "Graphical passwords using images with random tracks of geometric shapes," 2008 Congress on Images and Signal Processing. 2008

[2] P. Golle, ―Machine learning attacks against the Asirra CAPTCHA,in Proc. ACM CCS, 2008, pp. 535–542.

[3] Rosa Lin,Shih-Yu Huang, Graeme B Bell, Yeuan-Kuen Lee "A New CAPTCHA Interface Design for Mobile Devices" Australian computer society AUIC, 2011.

[4] Bin B. Zhu, Jeff Yan, Qiujie Li, Chao Yang, Jia Liu, NingXu, Meng Yi, KaiweiCai "Attacks and Design of Image Recognition CAPTCHAs" ACM, 2010.

[5] Niket Kumar Choudhary, Rahul Patil "CAPTCHAs based on the Principle- Hard to Separate Text from Background" vol. 5, 2014.

[6] Shubhangi G.Hande, M.S. Ali "enhancing the security using CAPTCHA as a Graphical Password" IJARCSMS, April, 2015.

[7] R.Biddle, S. Chiasson "Graphical Password: learning from the first twelve years" ACM, 2012

[8] H.Tao, C.Adams "PassGo: a proposal to improve the usability of graphical password" int J. Network, 2008.

[9] Ian jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin, USENIX Security Symposium August 23-36, 1999, Washington, D.C.

[10] Saranya Ramanan1, Bindhu J S "a survey on different graphical password authentication schemes"IJIRCEVol. 2, Issue 12, December 2014.