IJCSEC- International Journal of Computer Science and Engineering Communications.
Vol.3, Issue 2, 2015, Page.657-662, ISSN: 2347–8586

Graphical Password Authentication Using for Multistage Image Recognition Captcha

M.Anitha[1], B.Mahalakshmi[2],
PG Scholar, ME-CSE,
anithamurugaiyan91@gmai.com, rbmaha21@gmail.com
Sir Issac Newton College of Engineering and Technology, Nagapattinam.
Anna University Chennai, India.

ABSTRACT

Many security primitives are based on hard mathematical problems. One the problem use of passwords is a major point of vulnerability in computer security, as passwords are often easy to guess by automated programs running dictionary attacks. Passwords remain the most widely used authentication method despite their well-known security weaknesses. CAPTCHA authentication is clearly a practical problem. In a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology is call Captcha as graphical passwords. CaRP is both a Captcha and a graphical password scheme the authentication scheme that preserves the advantages of conventional password authentication. The proposed scheme is easy to implement and overcomes some of the difficulties of previously suggested methods of improving the security of user authentication schemes CaRP also offers protection against relay attacks, an increasing threat to bypass Captchas protection. An artificial image which contains some vital information, able to observe by Human but not by computer as automated task, is known as CAPTCHA image. The captcha will be used to prevent the task automation in performing repeated re try task in authentication process. The proposed scheme CAPTCHA also provides better protection against denial of service attacks against user accounts.

General Terms: Security, Human factors, Design, Experimentation.

Key Terms: Graphical password, password, hotspots, CaRP, Captcha, dictionary attack, password guessing attack, security Primitive.

1.INTRODUCTION

1.1 OVERVIEW

Passwords are the most common method of authenticating users, and will most likely continue to be widely used for the foreseeable future, due to their convenience and practicality for service providers and end users. Although more secure authentication schemes have been suggested in the past, using smartcards or public key cryptography, none of them has been in widespread use in the consumer market. The well-known problem in computer security that human chosen Passwords are inherently insecure since a large fraction of the users chooses passwords that come from a small domain. Security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. A small password domain enables adversaries to attempt to login to accounts by trying all possible passwords, until they find the correct one. This attack is known as a dictionary attack.

1.2 OBJECTIVE

Successful dictionary attacks have been recently reported against eBay user accounts, where attackers broke into accounts of sellers with good reputations in order to conduct fraudulent auctions. In addition to workstation and web log-in applications, graphical passwords have also been applied to many devices. CAPTCHA secure to protect the online email and password using for images. The present exemplary CaRPs built on both texts Captcha and image recognition Captcha. One of them is a text CaRP where in a password is a sequence of characters like a text password, but entered by clicking the right character sequence on CaRP images. CaRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services. Graphical password scheme may exceed that of text based schemes and thus presumably offer better resistance to dictionary attacks.

1.3 ABOUT THE PROJECT

Global password attacks consider a system that has many user accounts, and which enables logins over a network that is accessible to hackers. Again, do not assume that the attackers can sniff network traffic, only that they can connect to the network and try to login to the server, pretending to be a legitimate user. Consider an attacker that is interested in breaking into any account in the system, rather than targeting a specific account. The attacker can try many login attempts in parallel and circumvent the timing measure using the fact that user logins are typically handled by servers that can handle many login sessions in parallel. For example, the attacker can send a login attempt every 10 milliseconds, obtaining a throughput of 100 login attempts per second, regardless of how long the server delays the answers to the login attempts. The account locking feature can also be circumvented by such a global attacker, if it tries to login using different username and password pairs, and operates without trying the same user name twice. Since every user name is used only once, the account with many failed login attempts alarm is never triggered. Denial of service attacks the account locking feature enables denial of service attacks against users. These attacks are mounted by trying to login several times to a user's account with invalid passwords, thus causing this account to be blocked. For example, the report that users compete in auctions use these methods to block the accounts of other users competes in the same auctions.

2. LITERATURE SURVEY

2.1 PASS GO USABILITY

Adams. C et al.,[1] Inspired by an old Chinese game, Pass Go, designed a new graphical password scheme, in which a user selects intersections on a grid as a way to input a password. While offering an extremely large full password space 256 bits for the most basic scheme, the scheme provides acceptable usability, as empirically demonstrated by, to the best of our knowledge, the largest user study 167 subjects involved on graphical passwords, conducted in the fall semester of 2005 in two university classes. The scheme supports most application environments and input devices, rather than being limited to small mobile devices, and can be used to derive cryptographic keys. The memorable password space and show the potential power of this scheme by exploring further improvements and variation mechanisms.

2.2 SPYWARE USING CAPTCHA

Aickelin.U et al.,[2] discussed captcha, an automated test that humans can pass, but current computer programs can't pass any program that has high success over a captcha can be used to solve an unsolved Artificial Intelligence problem. The provide several novel constructions of captchas. Since captchas have many applications in practical security, this approach introduces a new class of hard problems that can be exploited for security purposes. Much like research in cryptography has had a positive impact on algorithms for factoring and discrete log, the hope that the use of hard AI problems for security purposes allows to advance the field of Artificial Intelligence. The robustness of CAPTCHA is found in its strength in resisting automatic adversarial attacks, automatic adversarial attacks, and it has many applications for practical security, including online polls, free email services, search engine bots, worms and spam, and preventing dictionary attacks .The proposal creates an innovative use of CAPTCHA in the context of graphical passwords to provide better password protection against spyware attacks.

2.3 PERSUASIVE CUED CLICK POINTS

Biddle . R et al., [3] described about the despite the ubiquity of password systems, knowledge-based authentication mechanism remains an important and active research area. Many current systems have low level security, and even then users often devise insecure coping strategies in order to compensate for memorability and usability problems. Alternatives such as tokens or biometrics raise other issues such as privacy and loss. Various graphical password mechanisms have received considerable attention in response. A systematic review of the literature on graphical passwords shows no consistency in the usability and security evaluation of various schemes. The situation is similar for text passwords, making fair comparison between methods nearly impossible.

2.4 SCHEME AGAINST SPYWARE

Dai.R et al., [4] discussed Text-based password schemes have inherent security and usability problems, leading to the development of graphical password schemes. However, most of these alternate schemes are Vulnerable to spyware attacks. The scheme is easy for humans but makes it almost impossible for automated programs to harvest passwords. The proposed a new authentication scheme combining graphical passwords with text based CAPTCHA. The scheme is easy for humans but makes it almost impossible for automated programs to harvest passwords. The novel scheme is friendly for legitimate users, while simultaneously raising the time and computer capacity cost to adversaries by several orders of magnitude. Experiments showed its effectiveness, but also indicated further research would improve its usability. Commonly, a spyware is a software that, from a user's perspective, covertly gathers information about a computer's use and relays that information back to a third party. Spyware has gradually become one of the most common security threats to computer systems. Password collection by spywares has rapidly increased 4, 5, 12, 13, and 15. The research community has expended much effort 4, 16, 17, 18, 20, 26 on this topic.

2.5 MODELING PASS POINTS

Dirik A. E et al., [5] discussed the model to identify the most likely regions for users to click in order to create graphical passwords in the Pass Points system. A Pass Points password is a sequence of points, chosen by a user in an image that is displayed on the screen. The model predicts probabilities of likely click points this enables us to predict the entropy of a click point in a graphical password for a given image. The model lows us to evaluate automatically whether a given image is well suited for the Pass Points system, and to analyze possible dictionary attacks against the system. The compare the predictions provided by the model to results of experiments involving human users. At this stage, the model and the experiments are small and limited but they show that user choice can be modeled and that expansions of the model and the experiments are a promising direction of research.

2.6 DRAW-A-SECRET METHOD

Dunphy.P et al., [6] discussed the common place text-based password schemes, users typically choose passwords that are easy to recall, exhibit patterns, and are thus vulnerable to brute-force dictionary attacks. This leads us to ask whether other types of passwords are also vulnerable to dictionary attack due to users tending to choose memorable passwords. The method to predict and model a number of such classes for systems where passwords are created solely from a user's memory. The hypothesize that these classes define weak password subspaces suitable for an attack dictionary. For user-drawn graphical passwords, the apply this method with cognitive studies on visual recall. These cognitive studies motivate us to define a set of password complexity factors, which define a set of classes.

2.7 MACHINE LEARNING ATTACKS

Gole.P et al., [7] described a classier which is 82:7% accurate in telling apart the images of cats and dogs used in Asirra. This classier is a combination of support-vector machine classiers trained on color and texture features extracted from images. The classier allows us to solve a 12 image Asirra challenge automatically with probability 10:3%. This probability of success is signicantly higher than the estimate of 0:2% given in for machine vision attacks. The results suggest caution against deploying Asirra without safeguards. The investigate the impact of the attacks on the partial credit and token bucket algorithms proposed. The partial credit algorithm weakens Asirra considerably and the recommend against its use. The token bucket algorithm helps mitigate the impact of the attacks and allows Asirra to be deployed in a way that maintains an appealing balance between usability and security. One contribution of our work is to inform the choice of safeguard parameters in Asirra deployments.

2.8 SECURE WEB APPLICATIONS

Kirda.E et al., [8] discussed that Authentication is the process of determining whether a user should be allowed to access to a particular system or resource. User can't remember strong password easily and the passwords that can be remembered are easy to guess. A password authentication system should encourage

strong and less predictable passwords while maintaining memorability and security. This password authentication system allows user choice while influencing users towards stronger passwords. The task of selecting weak password is more tedious, avoids users from making such choices. In effect, this authentication schemes makes choosing a more secure password the path of least resistance. Rather than increasing the burden on users, it is easier to follow the system's suggestions for a secure password a feature absent in most schemes. A password consists of one click-point per image for a sequence of images. The next image displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in. CCP offers both improved usability and security.

3. EXISTING SYSTEM

AI Fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. For example, the problem of integer factorization is fundamental to the RSA public-key cryptosystem and the Rabin encryption. The discrete logarithm problem is fundamental to the ElGamal encryption, the Diffie- Hellman key exchange, the Digital Signature Algorithm, the elliptic curve cryptography and so on. A recognition-based scheme requires identifying among decoys the visual objects belonging to a password portfolio. A typical scheme is Pass faces in a user select a portfolio of faces from a database in creating a password. During authentication, a panel of candidate faces is presented for the user to select the face belonging to her portfolio. This process is repeated several rounds, each round with a different panel. A successful login requires correct selection in each round. A successful login requires correct selection in each round. The set of images in a panel remains the same between logins, but their locations are permuted. Story is similar to pass faces but the images in the portfolio are ordered, and a user must identify her portfolio images in the correct order. Cognitive Authentication requires a user to generate a path through a panel of images as follows starting from the top-left image, moving down if the image is in her portfolio, or right otherwise. The user identifies among decoys the row or column label that the path ends.

4. PROPOSED SYSTEM

In the proposed system presents a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords. CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder surfing attacks. Notably, a CaRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. CaRP also offers a novel approach to address the well-known image hotspot problem in popular graphical password systems, such as Pass Points, that often leads to weak password choices. CaRP is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security. CaRP also offers protection against relay attacks, an increasing threat to bypass Captchas protection.Captcha can be circumvented through relay attacks there by Captcha challenges are relayed to human solvers and the answers are fed back to the targeted application.

5. PROBLEM DESCRIPTION

The most common computer authentication method is to use alphanumerical user names and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, some researchers have developed authentication methods that use pictures as passwords. In this project, conduct a comprehensive survey of the existing graphical password techniques. Classify these techniques into two categories recognition-based and recall-based approaches. Discuss the strengths and limitations of each method and point out the future research directions in this area.

6. AUTHENTICATION METHODS

Human factors are often considered the weakest link in a computer security system. Point out that there are three major areas where human computer interaction is important authentication, security, operations, and

developing secure systems. Current authentication methods can be divided into, three main areas Token based authentication, Biometric based authentication, Knowledge based authentication Graphical method for recall and recongtion based for the techniques, the recongtion based method for pured recall and cued recall method, this cued recall generate for image. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that created or selected earlier during the registration stage.

6.1 Token based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number.

6.2. Biometric based authentication

Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security.

6.3 Knowledge based authentication

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage.

7. RECOGNITION BASED CAPTCHA

Dhamija and Perrig proposed a graphical authentication scheme based on the Hash Visualization technique. In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program. Later, the user will be required to identify the pre selected images in order to be authenticated. The results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and pins. The average log-in time, however, is longer than the traditional approach. The regconition based method using the number of the random pictures and drawn the lines effect apperences created for the method. The images updated of the certain position and the authenticated for the every images for the log in the time.

8. MULTISTAGE IMAGE CAPTCHA

The CbPA-protocol in requires valid pair of user ID and password unless a valid browser cookie is received. Multistage image recognized method used for the captcha authentication

8.1FIRST CLICK VIEW

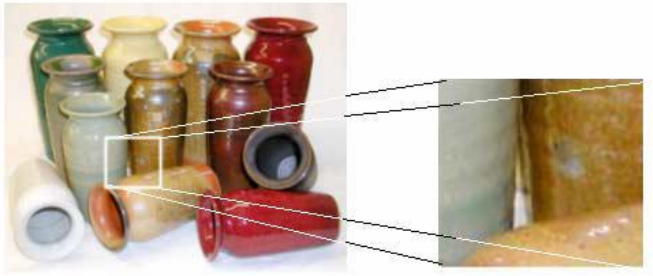
The first image captcha is the circled shaped using the cued click points for the method. The image rotated for various shaped in the x axis and y axis click point for the using .

8.2SECOND CLICK VIEW

The same as point cued click for the diamond shaped using for the captcha

8.3THIRED CLICK VIEW

The thired click poind some different view to the tracked point of the rectangled view to the image.



9.CONCLUSION

The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. To address this problem, some researchers have developed authentication methods that use pictures as passwords. In this project, conducted a comprehensive survey of existing graphical password techniques. The current graphical password techniques can be classified into two categories recognition-based and recall-based techniques. Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument.

10.REFERENCES

1. Adams.C et al., (2008), 'Pass-Go: A proposal to improve the usability of graphical passwords' Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292.
2. Aickelin.U et al.,(2010),'Against spyware using CAPTCHA in graphical password scheme' in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl., Jun, pp. 1–9.
3. Biddle .R et al.,(2008), 'Influencing users towards better passwords: Persuasive cued click-points' in Proc.Brit. HCI Group Annu. Conf. vol. 1., pp. 121–130.
4. Dai.R et al.,(2009), 'A new graphical password scheme against spyware by using CAPTCHA' in Proc. Symp. Usable Privacy Security, 2009, pp. 760–767
5. Dirik A. E et al., (2007), 'Modeling user choice in the pass points graphical password scheme' in Proc.Symp.Usable Privacy Security, pp.20–28.
6. Dunphy.P et al.,(2007), 'Do background images improve Draw a Secret graphical passwords' in Proc. ACM CCS, pp. 1–12.
7. Golle.P et al.,(2008), 'Machine learning attacks against the Asirra CAPTCHA' in Proc. ACM CCS, pp. 535–542.
8. Kirda.E et al.,(2007), 'Secure input for web applications Cued Click Point Technique for Graphical Password Authentication' in Proc. ACSAC, pp. 375–384.
9. Motoyama.M et al.,(2010), 'Re: CAPTCHAs —Understanding CAPTCHA solving services in an Economic Context' in Proc. USENIX Security,pp.23-28
10. Moy.M et al.,(2004), 'Distortion estimation techniques in solving visualCAPTCHAs' in Proc.Soc.Conf.Comput.Vis. Pattern Recognit., Jul, pp.23– 28.