SIR M VISVESVARAYA INSTITUTE OF TECHNOLOGY

BANGALORE- 562157

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING



**CAPTCHA AS GRAPHICAL PASSWORDS - A NEW SECURITY PRIMITIVE BASED ON HARD AI PROBLEMS**

Synopsis submitted

By

1. Samartha KV (1MV10CS092)
2. Manu K (1MV11CS408)
3. Vijesh Krishna (1MV10CS419)

Preferred Guide: Manjunath H C (Asst. Prof)

1. **INTRODUCTION**

Toda Security awareness is an important factor in an information security program. While organizations and institutes expand their use of advanced security technology and continuously train their security professionals, fraction of it is used to increase the security awareness among the normal users. As a result, today, organized cyber criminals are trying hard towards research and development of advanced hacking methods that can be used to steal money and secured information from the general public. Password authentication is one of the most common building blocks in implementing access control. Each user has a relatively short sequence of characters commonly referred to as a password. To gain access, providing right password is essential. Common attack for breaking password authenticated systems is dictionary attack. Graphical password is an option for alphanumeric password as text password is slightly hard to remember text password. When any application is provided with user friendly authentication it becomes easy to break and use that application. Cloud security can also be given by alphanumeric password but thing matter is that use of alphanumeric is not that much of secure and easy to remember. Any individual examining the password can memorize it which may lead to its misuse.

Graphical password schemes are more reliable and more resilient to dictionary attacks than textual passwords, but more vulnerable to shoulder surfing attacks. CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) is a program that generates and grades tests that are human solvable, but current computer programs do not have the ability to solve them. The robustness of Captcha is found in its strength in resisting automatic adversarial attacks, and it has many applications for practical security, including free email services, online polls, search engine bots, preventing dictionary attacks, worms and spam. CaRP is a combination of both a Captcha and a graphical password scheme. CaRP overcome a number of security issues, such as relay attacks, online guessing attacks, and, if combined with Captcha and graphical password, shoulder-surfing attacks. CaRP is click-based graphical passwords, where order of clicks on an image is used to get a new password. Unlike other click-based graphical passwords, images used in CaRP are used to generate Captcha challenges, and for every login attempt a new CaRP image is generated whether the existing user tries authenticating or a new user. In this paper we conduct a comprehensive survey of existing CaRP techniques namely Click Text, Click Animal and Animal Grid. We point out research direction in this area. We also try to answer our CaRP as secured as graphical passwords and text based passwords. Survey will be useful for information security researchers and practitioners who are interested in finding an alternative to graphical authentication methods.

Many security primitives are based on hard mathematical problems.  
Using hard AI problems for security is emerging as an exciting new paradigm, but has been underexplored. In this paper, we present 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. Captcha as graphical password is both a Captcha and a graphical password scheme. Captcha as graphical password 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 Captcha as graphical password password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. Captcha as graphical password 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. Captcha as graphical password is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security. Existing System Security primitives are based on hard mathematical problems.

A fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. This paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications. Using hard AI problems for security, initially proposed in, is an exciting new paradigm. Under this paradigm, the most notable primitive invented is Captcha, which distinguishes human users from computers.

1. **LITERATURE SURVEY**

In the current challenges facing technology, the encryption challenge has become a major point of concern. The utilization of text-in- image predicated security checks has availed to reduce fraud, but it’s not in its optimal efficiency. Looking to the future, we can visually perceive that for advanced transactions, mobile SMS verification and text predicated captchas are not enough. Hence we require coming up with an incipient scheme of security, which involves images and security primitives that are predicated on hard mathematical quandaries. Utilizing hard AI quandaries for security is emerging as an exhilarating incipient paradigm, but has been underexplored. The rudimentary task in security is to engender cryptographic primitives predicated on hard mathematical quandaries that are computationally intractable.

Albeit the proposed system may not be a hundred percent efficient approach, we are sure that it will surmount the current drawbacks being faced in internet transactions. The proposed system is an endeavour at simplifying the process of online payments or bank transfers etc. If implemented prosperously, this scheme may provide maximum security. The scope for future video-predicated sanctions withal amplifies.

**Disadvantages**

1. This paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications.
2. Using hard AI (Artificial Intelligence) problems for security, initially proposed before, is an exciting new paradigm. Under this paradigm, the most notable primitive invented is Captcha, which distinguishes human users from computers by presenting a challenge.
3. **PROPOSED MODEL:**

We present an incipient security primitive predicated on hard AI quandaries, namely, a novel family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CRP). Captcha as graphical password is both a Captcha and a graphical password scheme. Captcha as graphical password addresses a number of security quandaries altogether, such as online conjecturing attacks, relay attacks, and, if cumulated with dual-view technologies, shoulder-surfing attacks. Eminently, a Captcha as graphical password password can be found only probabilistically by automatic online conjecturing attacks even if the password is in the search set. Captcha as graphical password withal offers a novel approach to address the well-kenned image hotspot quandary in popular graphical password systems, such as Pass Points, that often leads to impuissant password culls. Captcha as graphical password is not a panacea, but it offers plausible security and usability and appears to fit well with some practical applications for amending online security.

We present exemplary Captcha as graphical passwords built on both text Captcha and image-apperception Captcha. One of them is a text Captcha as graphical password wherein a password is a sequence of characters like a text password, but entered by clicking the right character sequence on Captcha as graphical password images. Captcha as graphical password offers aegis against online dictionary attacks on passwords, which have been for long time a major security threat for sundry online accommodations. This threat is widespread and considered as a top cyber security peril. Bulwark against online dictionary attacks is a more subtle quandary than it might appear.

**Advantages:**

1. It offers reasonable security and usability and appears to fit well with some practical applications for improving online security.
2. This threat is widespread and considered as a top cyber security risk. Defence against online dictionary attacks is a more subtle problem than it might appear.

**Implementation:**

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it’s constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

**Main Modules:-**

**1. Graphical Password:**

In this module, Users are having authentication and security to access the detail which is presented in the Image system. Before accessing or searching the details user should have the account in that otherwise they should register first.

**2. Captcha in Authentication:**

It was introduced to use both Captcha and password in a user authentication protocol, which we call *Captcha-based Password Authentication (CbPA) protocol*, to counter online dictionary attacks. The CbPA-protocol in requires solving a Captcha challenge after inputting a valid pair of user ID and password unless a valid browser cookie is received. For an invalid pair of user ID and password, the user has a certain probability to solve a Captcha challenge before being denied access.

**3. Thwart Guessing Attacks:**

In a guessing attack, a password guess tested in an unsuccessful trial is determined wrong and excluded from subsequent trials. The number of undetermined password guesses decreases with more trials, leading to a better chance of finding the password. To counter guessing attacks, traditional approaches in designing graphical passwords aim at increasing the effective password space to make passwords harder to guess and thus require more trials. No matter how secure a graphical password scheme is, the password can always be found by a brute force attack. In this paper, we distinguish two types of guessing attacks: *automatic guessing attacks* apply an automatic trial and error process but *S* can be manually constructed whereas *human guessing attacks* apply a manual trial and error process.

**4. Security of Underlying Captcha:**

Computational intractability in recognizing objects in CaRP images is fundamental to CaRP. Existing analyses on Captcha security were mostly case by case or used an approximate process. No theoretic security model has been established yet. Object segmentation is considered as a computationally expensive, combinatorial-hard problem, which modern text Captcha schemes rely on.

**4. HARDWARE AND SOFTWARE REQUIREMENTS**

**4.1 Hardware requirements:**

* Processor type : Pentium 4
* Speed : 1.7 GHz
* Ram : 512MB
* Hard Disk : 40GB
* Keyboard : Standard

**4.2 Software requirements:**

* Operating System : Windows95/98/2000/XP
* Application Server : Tomcat5.0/6.X
* Front End : HTML, Java, Jsp
* Scripts : JavaScript.
* Server side Script : Java Server Pages.
* Database : Mysql 5.0
* Database Connectivity : JDBC.

**5. CONCLUSIONS:**

From the above project details, we can conclude that security is a difficult task. Today many security primitives are based on hard mathematical problems. Using hard AI problems for security is emerging as an exciting new paradigm, but has been underexplored. Captcha as graphical password addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. Captcha as graphical password is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security. Existing System Security primitives are based on hard mathematical problems. A fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. Using hard AI problems for security is new approach and will soon be widely accepted and used.

**6. REFERENCES:**

WEBSITES:

1. [www.explore.ieee.org](http://www.explore.ieee.org)

2. [www.wikipedia.com](http://www.wikipedia.com)

BOOKS:

1. [Information Forensics and Security, IEEE Transactions on](http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206)  (Volume:9 ,  [Issue: 6](http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=6803967) ) 19 March 2014.
2. Liming Wang, Xiuling Chang, Zhongjie Ren, Haichang Gao, XiyangLiu, Uwe Aickelin, “Against Spyware Using CAPTCHA in Graphical Password Scheme”
3. [Zhu, B.B.](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Zhu,%20B.B..QT.&newsearch=true) Microsoft Res. Asia, Beijing, China [Yan, J.](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Yan,%20J..QT.&newsearch=true) ; [Guanbo Bao](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Guanbo%20Bao.QT.&newsearch=true) ; [Maowei Yang](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Maowei%20Yang.QT.&newsearch=true) ; [Ning Xu](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Ning%20Xu.QT.&newsearch=true)
4. Matthew Dailey, Chanathip Namprempre,“A Text-Graphics Character CAPTCHA for Password Authentication.