ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Enhanced User Security Using Graphical Passwords

Soujanya Koorapati
MTech Student
Department of CSE
Talla Padmavathi College of Engineering

Vishnu Vardhan Sarva
Assistant Professor
Department of CSE
Talla Padmavathi College of Engineering

Abstract: ***Online security is a tree branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing. Different methods have been used to protect the transfer of data, including encryption. This paper works on image based captcha to protect user data or unauthorized access of information. In that password is created from images and text password. Current system is based on only text password but it has disadvantages small password mostly used and easy to remember. This type of password is easy to guess through different attack i.e. dictionary attack and brute force attack. In this paper we have proposed a new image password scheme. In this Recognition based technique is used with numerical password which provide more security and easy to remember text and graphical password.***

Keywords: ***Online Security, Captcha, Password, Encryption, Graphical Images, Brute force***

Introduction: Today, computer theft and data loss are growing problems for consumers as well as businesses, small to large. As more and more of our important documents, personal information and financial data are stored on computers, our diligence has to improve and security solutions have to evolve to provide better protection or we risk losing some or all of it to criminals, competitors, enemies or others who should not have access.

These days we do everything online, our computers, laptops and smartphones have become an extension of ourselves so ensuring we have the best internet security is a way of knowing that our identities, documents and passwords are not compromised. With the internet came a selection of fraudulent activities from identity thieves to people who hack computers and steal private passwords, documents and files. The fact we do everything online only opens us up to these frauds and makes us sitting victims, unless you have taken the necessary steps to protect your computer to the best of your ability.

It still surprises me how many people don't bother with internet security. They seem to think that their computers are invisible, but as soon as you start using your computer for anything that involves logging onto the internet you are easy prey. The safest method is to buy good internet security software, a program that will immediately remove viruses, advice you when you are browsing the internet and click on a malicious site and one that does regular scans of your computer to detect any damaging materials which may compromise both you and your computer.

The starting point is that there is no absolute security. There will always be threats and vulnerabilities, so our concept of "secure" has to reflect that reality. We need

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

think about "secure" in terms of residual risks that are considered acceptable in a specific context. That is also why "resilience" is an important metric when defining the objective of Internet security efforts.

But the Internet, with its high degree of interconnection and dependencies, brings another dimension to the management of risks. Security and resilience of the Internet depends not only on how well risks to you and your assets are managed – the "inward" risks, but also, importantly, on the management of risks that you (by your action or inaction) present to the Internet ecosystem – the "outward" risks. Additionally, some risks need to be managed by more than one actor. This is the notion of collective and shared risk management – a notion that is well aligned with the "public interest" nature of the Internet.

A CAPTCHA (an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart") is a type of challenge-response test used in computing to determine whether or not the user is human.

The term was coined in 2003 by Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford. The most common type of CAPTCHA was first invented in 1997 by Mark D. Lillibridge, Martin Abadi, Krishna Bharat, and Andrei Z. Broder. This form of CAPTCHA requires that the user type the letters of a distorted image, sometimes with the addition of an obscured sequence of letters or digits that appears on the screen. Because the test is administered by a computer, in contrast to the standard Turing test that is administered by a human, a CAPTCHA is sometimes described as a reverse Turing test. This term is ambiguous because it could also mean a Turing test in which the participants are both attempting to prove they are the computer.

This user identification procedure has received many criticisms, especially from disabled people, but also from other people who feel that their everyday work is slowed down by distorted words that are illegible even for users with no disabilities at all.

CAPTCHAs are by definition fully automated, requiring little human maintenance or intervention to administer. This has obvious benefits in cost and reliability.

By definition, the algorithm used to create the CAPTCHA must be made public, though it may be covered by a patent. This is done to demonstrate that breaking it requires the solution to a difficult problem in the field of artificial intelligence (AI) rather than just the discovery of the (secret) algorithm, which could be obtained through reverse engineering or other means.

Modern text-based CAPTCHAS are designed such that they require the simultaneous use of three separate abilities—invariant recognition, segmentation, and parsing—to correctly complete the task with any consistency.

Invariant recognition refers to the ability to recognize the large amount of variation in the shapes of letters. There are nearly an infinite number of versions for each character that a human brain can successfully identify. The same is not true for a computer, and teaching it to recognize all those differing formations is an extremely challenging task.

Segmentation, or the ability to separate one letter from another, is also made difficult in CAPTCHAs, as characters are crowded together with no white space in between.

Context is also critical. The CAPTCHA must be understood holistically to correctly identify each character. For example, in one segment of a CAPTCHA, a letter might look like an "m." Only when the whole word is taken into context does it become clear that it is a "u" and an "n."

Computer character recognition

Although CAPTCHAs were originally designed to defeat standard OCR software designed for document

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

scanning, a number of research projects have proven that it is possible to defeat many CAPTCHAs with programs that are specifically tuned for a particular type of CAPTCHA. For CAPTCHAs with distorted letters, the approach typically consists of the following steps:

- Removal of background clutter, for example with color filters and detection of thin lines.
- Segmentation, i.e., splitting the image into segments containing a single letter.
- Identifying the letter for each segment.

Step 1 is typically very easy to do automatically. In 2005, it was also shown that neural network algorithms have a lower error rate than humans in step 3. The only part where humans still outperform computers is step 2. If the background clutter consists of shapes similar to letter shapes, and the letters are connected by this clutter, the segmentation becomes nearly impossible with current software. Hence, an effective CAPTCHA should focus on step 2, the segmentation.

Neural networks have been used with great success to defeat CAPTCHAs as they are generally indifferent to both affine and non-linear transformations. As they learn by example rather than through explicit coding, with appropriate tools very limited technical knowledge is required to defeat more complex CAPTCHAs.

Some CAPTCHA-defeating projects:

Mori et al. published a paper in IEEE CVPR'03 detailing a method for defeating one of the most popular CAPTCHAs, EZ-Gimpy, which was tested as being 92% accurate in defeating it. The same method was also shown to defeat the more complex and less-widely deployed Gimpy program 33% of the time. However, the existence of implementations of their algorithm in actual use is indeterminate at this time.

PWNtcha has made significant progress in defeating commonly used CAPTCHAs, which has contributed to a general migration towards more sophisticated CAPTCHAs.

A number of Microsoft Research papers describe how computer programs and humans cope with varying degrees of distortion.

Image recognition CAPTCHAs vs. character recognition CAPTCHAs

With the demonstration (through research publications) that character recognition CAPTCHAs are vulnerable to computer vision based attacks, some researchers have proposed alternatives to character recognition, in the form of image recognition CAPTCHAs which require users to identify simple objects in the images presented. The argument is that object recognition is typically considered a more challenging problem than character recognition, due to the limited domain of characters and digits in the English alphabet.

Some proposed image recognition CAPTCHAs include:

Chew et al. published their work in the 7th International Information Security Conference, ISC'04, proposing three different versions of image recognition CAPTCHAs, and validating the proposal with user studies. It is suggested that one of the versions, the anomaly CAPTCHA, is best with 100% of human users being able to pass an anomaly CAPTCHA with at least 90% probability in 42 seconds.

Datta et al. published their paper in the ACM Multimedia '05 Conference, named IMAGINATION (IMAge Generation for INternet AuthenticaTION), proposing a systematic way to image recognition CAPTCHAs. Images are distorted in such a way that state-of-the-art image recognition approaches (which are potential attack technologies) fail to recognize them.

Microsoft (Jeremy Elson, John R. Douceur, Jon Howell, and Jared Saul) have developed Animal Species Image Recognition for Restricting Access (ASIRRA) which ask users to distinguish cats from dogs. Microsoft had a beta version of this for websites to use. They claim "Asirra is easy for users; it can be solved by humans 99.6% of the time in under 30

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

seconds. Anecdotally, users seemed to find the experience of using Asirra much more enjoyable than a text-based CAPTCHA." This solution was described in a 2007 paper to Proceedings of 14th ACM Conference on Computer and Communications Security (CCSIts) However, this project was closed in October 2014 and is no longer available.

Existing System

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. **A** FUNDAMENTAL task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable.

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 in [17], 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.

Proposed System

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 (CaRP). 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 PassPoints, 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.We present exemplary CaRPs built on both text Captcha and image-recognition Captcha.

One of them is a text CaRP wherein 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. This threat is widespread and considered as a top cyber security risk. Defense against online dictionary attacks is a more subtle problem 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. Defense 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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

details user should have the account in that otherwise they should register first.

2. Captica in Authentication:

It was introduced in [14] 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 :

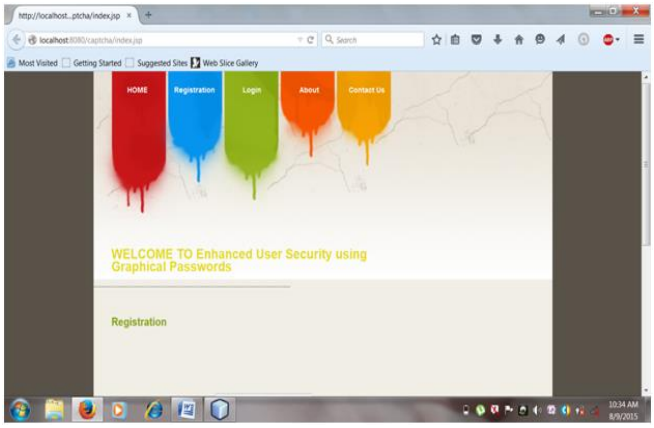
In a guessing attack, a password guess tested in an unsuccessful trial is determined wrong and excluded from subsequent trials. The number of undetermined password guesses decreases with more trials, leading to a better chance of finding the password. To counter guessing attacks, traditional approaches 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:

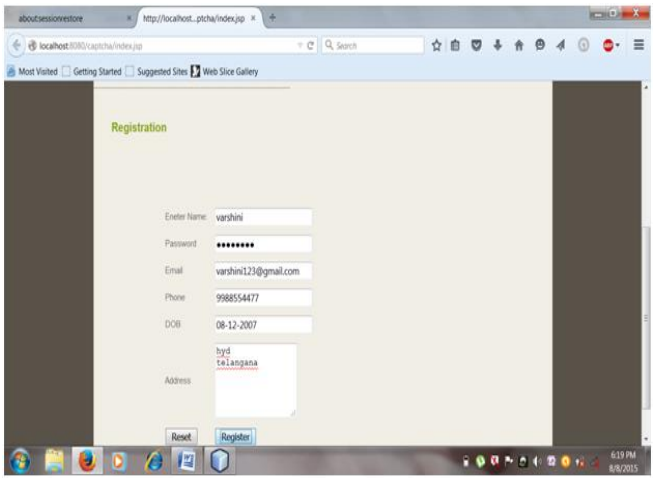
Computational intractability in recognizing objects in CaRP images is fundamental to CaRP. Existing analyses on Captcha security were mostly case by case or used an approximate process. No theoretic security model has been established yet. Object segmentation is considered as a computationally expensive,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

Screen Shots:

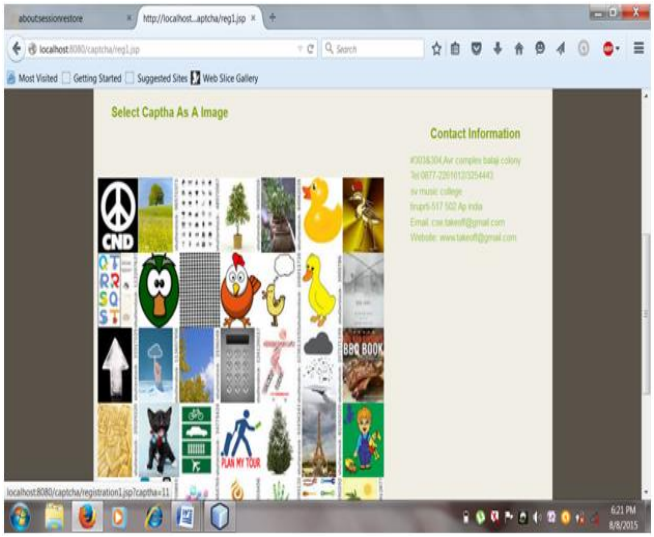
HOME PAGE



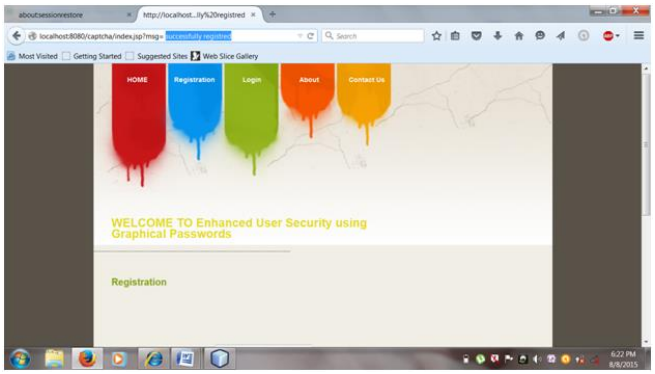
REGISTRATION



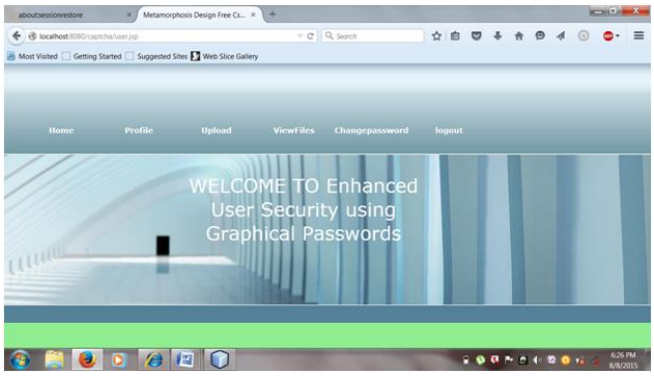
SELECT A CAPTCHA



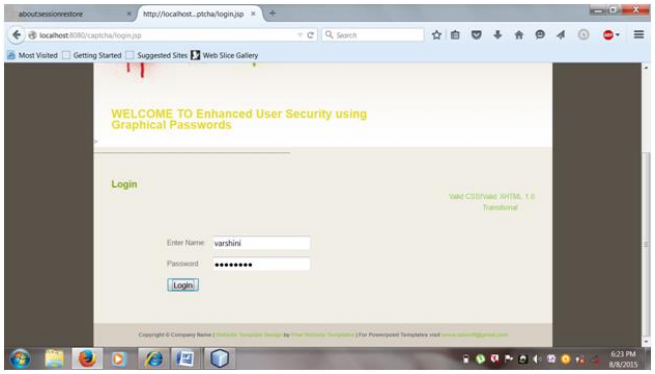
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



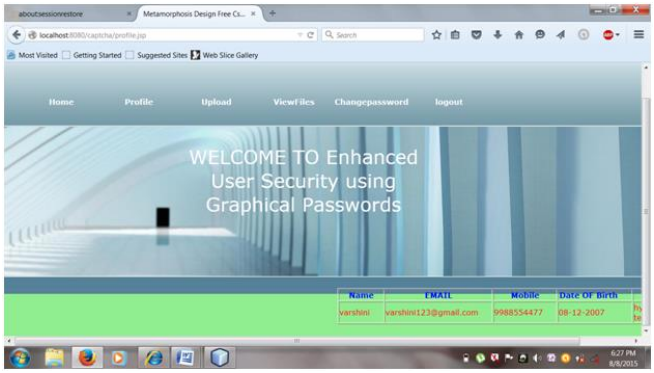
USER SUCCESSFULLY REGISTERED



LOGIN

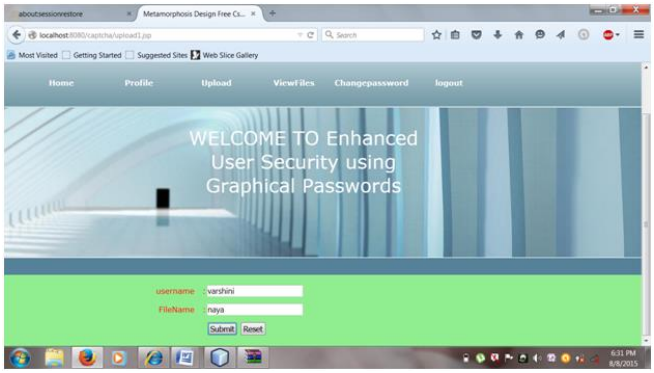


PROFILE

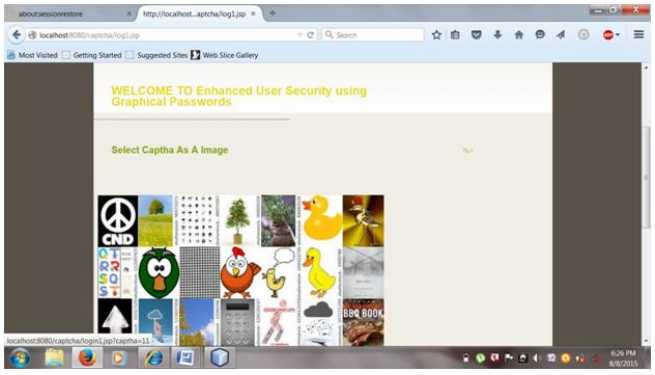


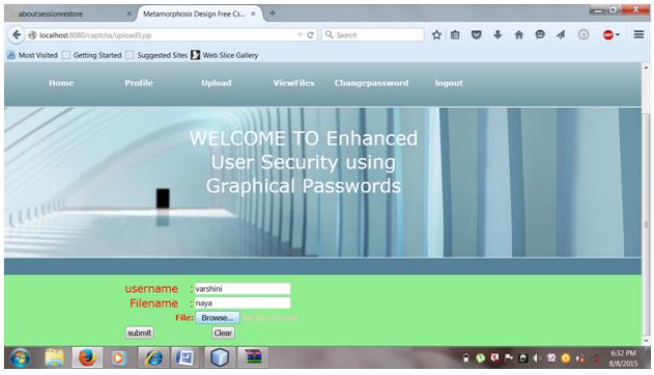
ENTER THE CAPTCHA

UPLOADING A FILE



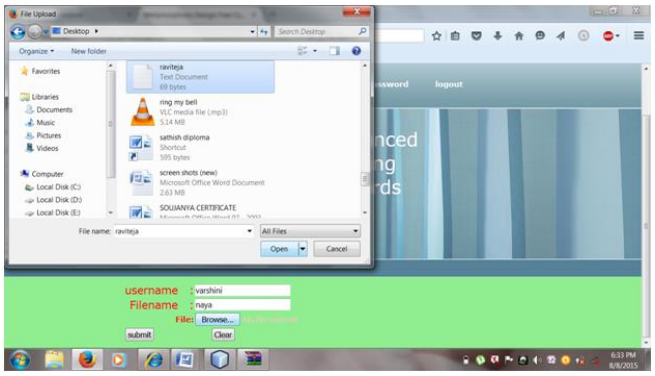
CLOSE CAPTCHA

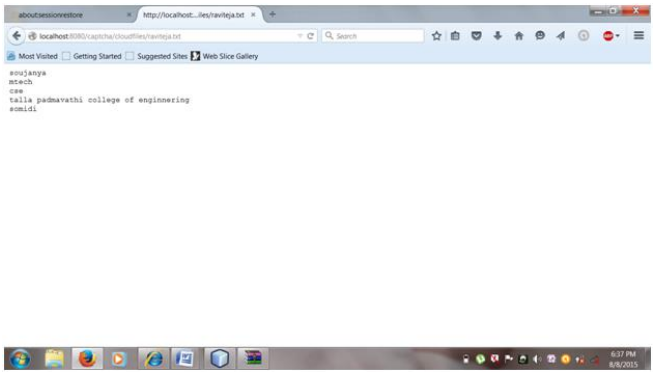




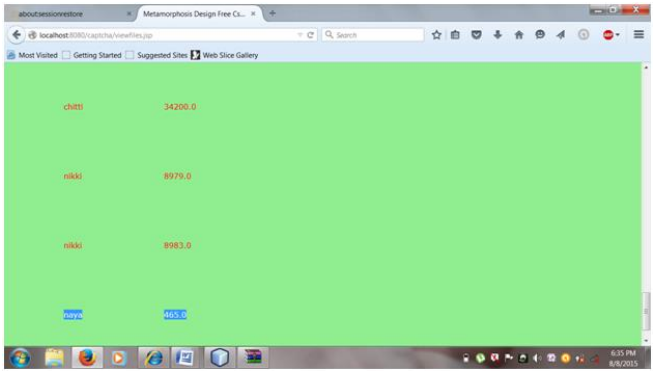
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

SELECT A FILE FROM THE COMPUTER

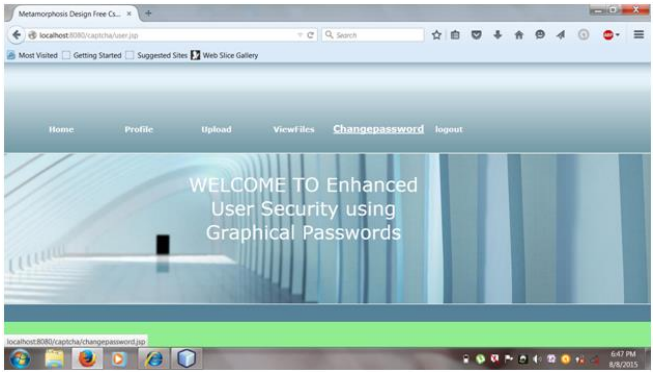




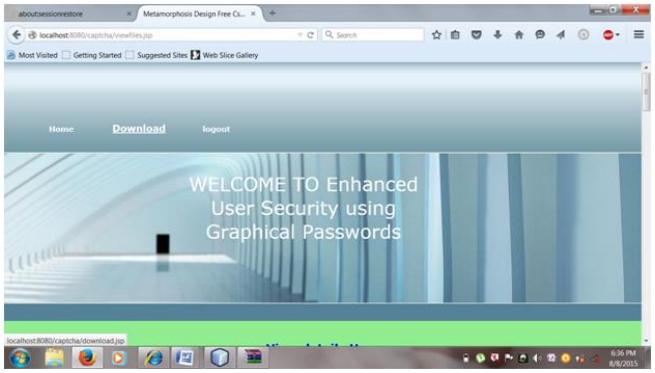
VIEW FILE DETAILS

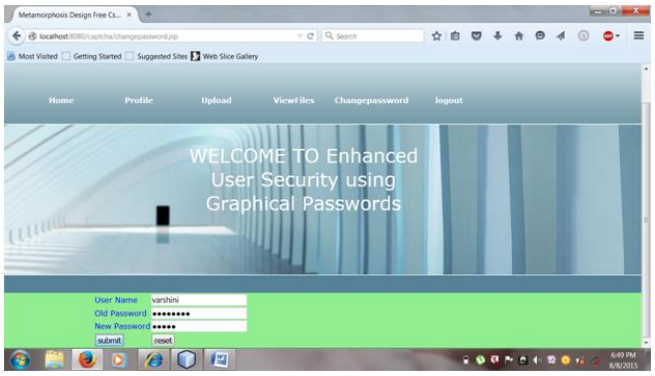


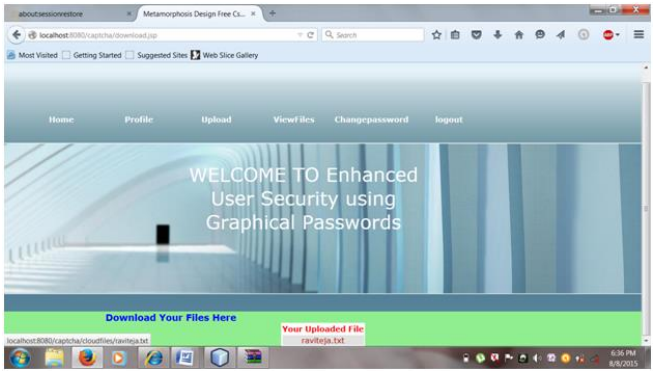
CHANGE PASSWORD

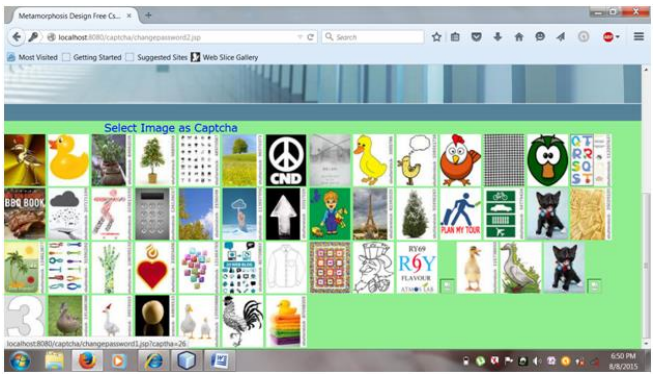


DOWNLOAD THE FILE

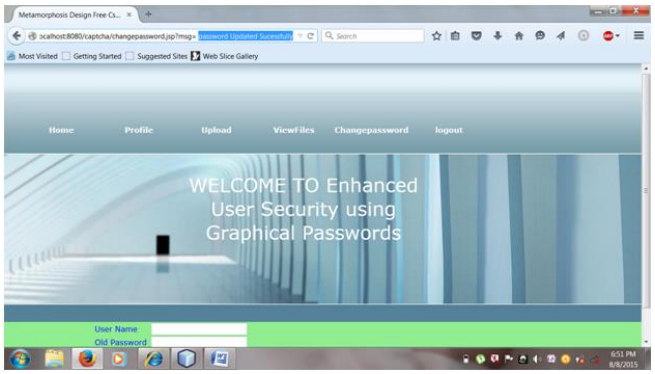




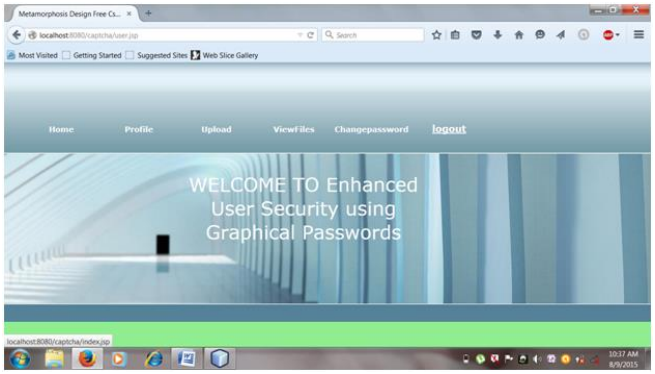




ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



LOGOUT



Conclusion: With the Internet now playing such an integral role in every aspect of business, from the cloud to mobile devices, security has never been a more important issue. With that in mind, this article looks at some of the most common security threats that a business can face and what you can do to protect your data and make your online activities safer. Our graphical password system provides more security to data and protection against different attack. Our graphical password system is based on text password and graphical password. For successful login user has to select correct image which is chosen by user during a registration and this system provide text password which provide more security to data. The paper studies and implements a comprehensive technique of CAPTCHA as Graphical Password schemes. CaRP is a combination of both a CAPTCHA and a graphical password scheme. CaRP schemes are classified as Recognition-Based CaRP and Recognition-Recall CaRP. We have discussed Recognition Based CaRP which include ClickText, ClickAnimal and AnimalGrid techniques in this paper. Current graphical password techniques are an alternative to text password but are still not fully secure. As a framework, CaRP does not rely on any specific CAPTCHA scheme. When one CAPTCHA scheme is broken, a new and more secure one may appear and be converted to a CaRP scheme. Due to reasonable security and usability and practical applications, CaRP has good potential for refinements. The usability of CaRP can be further improved by using images of different levels of difficulty based on the login history of the user and the machine used to log in.

References:

[1] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014

[2] Xiaoyuan Suo, Ying Zhu, G. Scott. Owen, "Graphical Passwords: A Survey", Department of Computer Science Georgia State University

[3] Matthew Dailey, Chanathip Namprempre,"A Text-Graphics Character CAPTCHA for Password Authentication"

[4] T. S. Ravi Kiran, Y. Rama Krishna, "Combining CAPTCHA and graphical passwords for user authentication" , International Journal of Research in IT & Management, Volume 2, Issue 4 (April 2012) (ISSN 2231-4334)

[5] Liming Wang, Xiuling Chang, Zhongjie Ren, Haichang Gao, Xiyang Liu, Uwe Aickelin, "Against Spyware Using CAPTCHA in Graphical Password Scheme"

[6] Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford, "CAPTCHA: Using Hard AI Problems For Security"

[7]Darryl D'Souza Phani, C.Polina, Roman V and Yampolskiy.Avatar Captcha: Telling Computers and humans apart via face classification.IEEE, 2012.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[8] Robert Biddle, Sonia Chiasson and P.C.van Oorschot. Graphical Passwords: Learning from the First Twelve Year. School of Computer Science, Carleton University, Jan 4, 2012.

[9] Mohamed Sylla, Gul Muhammad, Kaleem Habib and Jamaludin lbrahim.Combinatoric Drag-Pattern Graphical Password. Journal of Emerging Trends in Computing Information Sciences, Vol.4,No.12,Dec 2013.

[10] www.yuavengineers.com