Middle-East Journal of Scientific Research 24 (10): 3351-3357, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.3351.3357

A New Security Prespective-Authentication Procedure Integrating Captcha, Graphical Password and Soundmonogram

[1]M. Usha and [1]P. Prittopaul, [2]M. Keerthana and [2]M. Chellammaljayashree

[1]Asst. Professor, Department of CSE, Velammal Engineering College, India
[2]UG Scholar, Department of CSE, Velammal Engineering College, India

Abstract: Since the bloom of computer era and internet has been succeeding constantly so does its security issues. Till date 1 out of 10 (Approx.) becomes a victim of cyber-crimes. One such issue is password. There were many security primitives implemented to provide utmost security to the user. Some existing methods are biometric, pattern recognition, etc. But each and every method had ambiguities which made hacker to penetrate easily and finally underexplored. The most commonly used type of user authentication is text based authentication. This type of technology is easy to explore by the hacker using Denial of Service attack, Online Glossary attack. In this paper, we present a new security primitive based on AI problems, namely, a Nobel family of graphical password system built on the top of Captcha technology, which will be called as Captcha as graphical password (CaRP). CaRP is each a Captcha and a graphical watchword theme. This project incorporates the three kinds of technologies, CAPTCHA, Graphical passwords, sound monogram technique for efficient security primitive for the user.

Key words: CAPTCHA · Biometric · Patternrecognition · Graphical Password

INTRODUCTION

A Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) is a type of provocation – response test used in computing to distinguish whether the user is a human or not. The most common type of CAPTCHA method used till date which requires the user to type the letters of distorted image, sometimes addition to the letters it may also include numerical. In the CAPTCHA technique the test to distinguishing between the user and computer is done by another computer, thus sometimes CAPTCHA is best described as reverse Turing test. CAPTCHA is a fully automated and requires little human maintenance or intervention for administration. According to an article by Ahn, Blum and Langford "Any program that passes the test generated by CAPTCHA can be used to solve a hard unsolved AI problem."

Fig. 1.1: CAPTCHA password

Introduction to Graphical Password: A graphical password is a user based validation/authentication system that works by making the user to select a image, in a specific order, presented in GUI (Graphical User Interface). This type of authentication process sometimes called as GUA (Graphical User Authentication). Graphical password scheme was proposed to replace the text based authentication. In text based authentication process, people tend to type the text password followed by their user name. The problem of using the text based authentication increased substantially from time to time. The two main problems of text based authentications are said to be:

- Remembering the password
- Security risks (Online Dictionary attack, Denial Of Service attacks, etc)

Corresponding Author: M. Usha, Asst. Professor, Department of CSE, Velammal Engineering College, India.

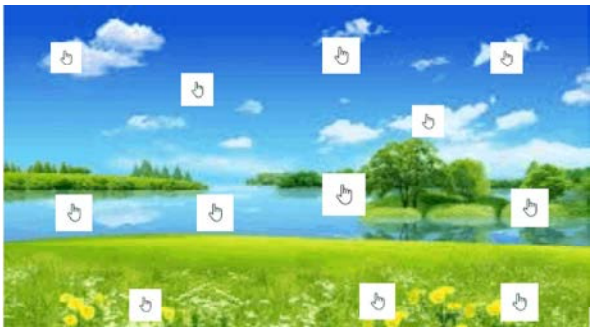

Fig. 1.2: Graphical Passwords

Characterstics of Captcha

- Fully automated
- Requires less human assistance
- Turing test capability
- Invariant recognition
- Segmentation
- Parsing

Characterstics of Graphical Password

- Freedom of choice
- Efficient
- Memorable
- Input Reliability and Accuracy
- Grid based
- Ease of use

APPLICATIONS

- Preventing comment spam in blogs
- Protecting online Registration
- Protecting e-mail from Scrapers
- Online polls
- Preventing dictionary attack
- Search Engine bots
- Worms and Spam
- Protects from Denial Of Service attack
- Protects from Dictionary attack

Literature Survey

Grid Resource Abstraction, Virtualization and Provisioning for Time-Targeted Applications: This Paper introduces a new HPDC resource management paradigm named, resource slot which defines a network of logical machines across time and space. A resource slot is not only a resource programming target but also a virtualized resource provisioning framework for a variety of resource management paradigms by encapsulating there source management complexity. Especially, we present a resource provisioning technique named guided redundant submission (GRS), which probabilistically guarantees a timely resource slot allocation.

Multiple Password Interference in Text Passwords and Click-based Graphical Passwords: Click-based graphical passwords were significantly less susceptible to multiple password interference in the short-term, while having comparable usability to text passwords in most other respects.

Comparing Passwords, Tokens and Biometrics for User Authentication: This paper examines passwords, security tokens and biometrics—which we collectively call authenticators—and compares these authenticators and their combinations. The paper endeavors to offer a comprehensive picture of user authentication solutions for the purposes of evaluating options for use and identifying deficiencies requiring further research.

Sequence Selection of Captcha as Graphical Password Schemeagainst Spyware: CAPTCHA as graphical passwords (CaRP) is a graphical password scheme used for a user access authentication. In this Paper, each and every scheme of CAPTCHA password like graphical password scheme and focus the security attitude and analysis the attack methods how to secure from attacks in the sequence selection of CaRP scheme against spyware.

Graphical Passwords as Browser Extension: Implementation and Usability Study: In this paper, GPEX, a password manager program implemented as a web browser plug-in to enable using graphical passwords to secure Internet applications without any need to change their authentication interface.

KLASSP: Entering Passwords on a Spyware Infected Machine Using a Shared Secret Proxy: In this paper,the problem of entering sensitive data were examined, such as password, from a trustless machine. By trustless we mean that it is suspected to be infected with spyware which snoops on the user's activity. Using such a machine is obviously undesirable and yet roaming users often have no choice. They are in no position to judge the security status of internet cafe, airport lounge or business center machines. Either malice or negligence on the part of an administrator means that any such machine can easily be running a key logger.

Existing System

- In the existing system, Brostoff and sasse carried out an empirical study of pass faces, which illustrates well how a graphical password recognition system typically operates.
- Blonder-style passwords are based on cued recall. A user clicks on several previously chosen locations in a single image to log in. As implemented by Passlogix Corporation, the user chooses several predefined regions in an image as his or her password.
- To log in the user has to click on the same regions in effect, cued click points (ccp) is a proposed alternative to passpoints.
- In ccp, users click one point on each of 5 images rather than on five points on one image.
- It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point (at which point they can cancel their attempt and retry from the beginning).
- It also makes attacks based on hotspot analysis more challenging.
- Each click results in showing a next-image, in Effect leading users down a "path" as they click on their sequence of points.
- A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click.
- Users can choose their images only to the extent that their click-point dictates the next image.
- While the predictability problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords.
- Number of graphical password systems have been developed, Study shows that text-based passwords suffers with both security and usability problems

Disadvantage

- The problem with this scheme is that the number of predefined regions is small, perhaps a few dozens in a picture.
- The password may have to be up to 12 clicks for adequate security, again tedious for the user.
- Another problem of this system is the need for the predefined regions to be readily identifiable.

Proposed System

- In the proposed work we have integrated sound monogram to help in recalling the password.
- No system has been devolved so far which uses soundmonogram in graphical password authentication.
- Study says that sound monogram or tone can be used to recall facts like images, text etc. In daily life we see various examples of recalling an object by the sound related to that object enters User ID and select one sound frequency which he want to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter.
- To create detailed vector user has to select sequence of images and clicks on each image at click points of his choice. Profile vector is created.

Advantage

- To create detailed vector user has to select sequence of images and clicks on each image at click points of his choice. Profile vector is created.
- Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image was easier and sound monogram helps considerably in recalling the click points.
- System showed very good Performance in terms of speed, accuracy and ease of use.

The simple architecture diagram explains the various phase of Proposed System:

- 1. Registering User Details
- 2. Upload User Desired Image
- 3. Login
- 4. OTP verification

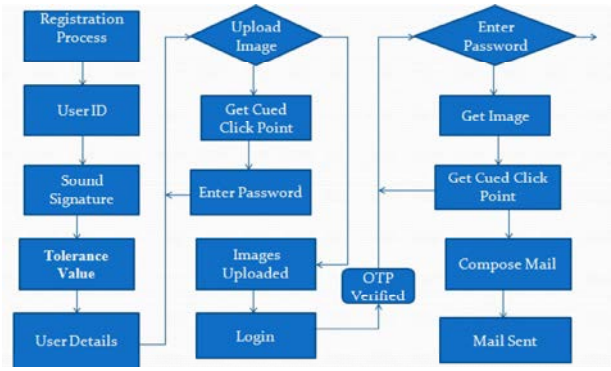

Fig. 6.1: System Architecture Diagram

System Implementation
List of Modules

- Click Patterns
- Tolerance Range
- Sound monogram
- Secure Recovery

Click Patterns: A precursor to PCCP, Cued Click-Points (CCP) was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Rather than five click-points on one image, CCP uses one click-point on five different images shown in sequence. The next image displayed is based on the location of the previously entered click-point, creating a path through an image set. Users select their images only to the extent that their click-point determines the next image. Creating a new password with different click-points results in a different image sequence.

Tolerance Range: After creation of the login vector, system calculates the Euclidian distance between login vector and profile vectors stored. Euclidian distance between two vectors p and q is given by-Above distance is calculated for each image if this distance comes out less than a tolerance value D. The value of D is decided according to the application. In our system this value is selected by the user. Tolerance level used for get coordinated pixels for our selected click points in our image.

Sound Monogram: Sound monogram is mainly added to solve guessing attack as we provide multiple click points from different images guessing attack will be happened. So we assigning a specific sound monogramfor cued click points which as been represented as graphical password. 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.

Secure Recovery: If user forgets the click points or frequent guessing attacks user was redirected to recovery phase where user allowed resetting their graphical passwords of same images or they can select graphical passwords from new images along with sound monogram. It mainly protect users from password re-usability.

Implementation Results
User Interface: In UI phase the registration process takes place. User fills in the required details and selects next to move to the next page.

Fig. 6.1: User Interface

Uploading the Image and Getting Cued Click Points: Image is uploaded using the viewport and pixel coordination algorithm. Getting cued click point sets the password for authentication.

Fig. 6.2: Image Uploading

Fig. 6.4: Cued Click Point

Password Protection for the Image& Uploading of Second Image: Each uploaded image should be protected with a text based authentication to provide high security. Each image has its own text based password. After this text based authentication of first image, it will lead to uploading of second image.

Fig. 6.5: Password for the image

Fig. 6.6: Upload Second Image

Upload Second Image and Get Cued Clickpoints: As performed for the first image, user uploads the second image and gets the cued click point and protects it with the text based password.

Fig. 6.7: Get Cued Click Points

Enter Password Protection: Password protection for the user uploaded second image are given to proceed to the next stage.

Fig. 6.8: Password For Second Image

LOGIN: After registration phase, user is navigated to login phase where he is asked to enter the userid.

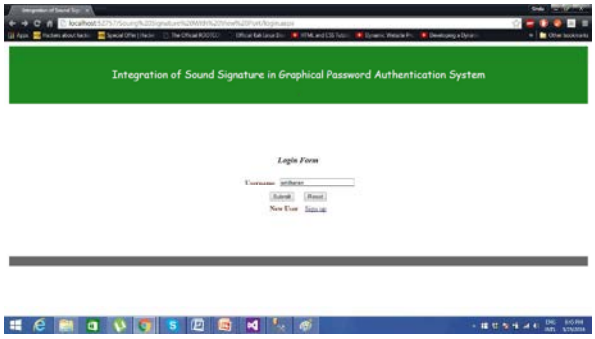

Fig. 6.9: Login

OTP Verification: OTP verification through mail provides the next step of security to the user to stop the unauthorized entry to some extent.

Fig. 6.10: OTP Verification

Enter the Passwordto Get Image: To get the user uploaded image during the registration phase, user has to enter the correct text based password.

Fig. 6.11: Password to Get Image

Enter the Password to Get the next Image: User perform the cud click point, if correct will play user selected sound frequency else it plays the random sound, making the un authorized user to get confused.

Fig. 6.12: Next Image Password

Final Login Page: After successful two cued click points in two user uploaded image,The user is finally navigated to his authenticated profile.

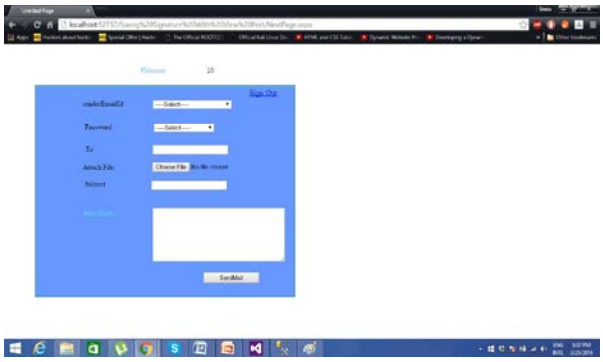

Fig. 6.13: Successful Login

CONCLUSION

Security primitive that is to be ensured in a password-based authentication systems is to maximize the effectiveness password usability. In our project we have ensured that it is possible to make user choice efficient meanwhile on other hand increasing the effective password usability. Moreover, highly specialized tools like PCCP's viewport (used during password creation) cannot be exploited easily at the time of attack. Users could be further deterred (at some cost in usability) from selecting obvious click-points by limiting the number of shuffles allowed during password creation or by progressively slowing system response in repositioning the viewport with every shuffle past a certain threshold. The various model schemes discussed in this paper present a clear distinguishing ground between insecure and memorable user-chosen (text based) passwords and secure system generated random passwords that are difficult to remember.

We have proposed CaRP scheme with incorporating sound monogram, a security primitive relying on unsolved hard AI problems. CaRP is both a CAPTCHA and a graphical password scheme. The sound monogram scheme is incorporated to notify the user whether his enterd password is correct or not. Each stage of cued click point from one image to other is secured by text based authentication. The next image appears only if the text authentication provided by the user is correct. The notion of CaRP introduces a new family of graphical passwords, which adopts a new approach to counter online guessing attacks: a new CaRP image, which is also a CAPTCHA challenge, is used for every login attempt to make trials of an online guessing attack computationally independent of each other. A password of CaRP can be found only probabilistically by automatic online guessing attacks including brute-force attacks, a desired security property that other graphical password schemes lack.

REFERENCES

1. Chiasson, S., R. Biddle and P. van Oorschot, 2007. A Second Look atthe Usability of Click-Based Graphical Passwords, Proc. ACMSymp. Usable Privacy and Security (SOUPS),
2. Chiasson, S., A. Forget, R. Biddle and P. van Oorschot, 2008. InfluencingUsers towards Better Passwords: Persuasive Cued Click-Points, Proc. British HCI Group Ann. Conf. People and Computers:Culture, Creativity, Interaction,
3. Chiasson, S., A. Forget, E. Stobert, P. van Oorschot and R. Biddle, 2009. Multiple Password Interference in Text and Click-Based GraphicalPasswords, Proc. ACM Conf. Computer and Comm. Security (CCS),
4. Stobert, E., A. Forget, S. Chiasson, P. van Oorschot and R. Biddle, 2010. Exploring Usability Effects of Increasing Security in Click-BasedGraphical Passwords, Proc. Ann. Computer Security Applications Conf. (ACSAC).
5. Chiasson, S., A. Forget, R. Biddle and P.C. van Oorschot, 2009. UserInterface Design Affects Security: Patterns in Click-Based Graphical Passwords, Int'l J. Information Security, 8(6): 387-398.