Password Security Based on CaRP using Hard AI Problem

Mr. Darekar Kishor[1] Mr. Sonawane Navin[2] Mr Shivale Kiran[3] Prof. Thakur R.B[4]
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]Institute of Knowledge College of Engineering, Pune

Abstract— Usable security has unique usability challenges because the need for security often means that standard human-computer-interaction approaches cannot be directly applied. An important usability goal for authentication systems is to support users in selecting better passwords. Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. So researchers of modern days have gone for alternative methods wherein graphical pictures are used as passwords. Graphical passwords essentially use images or representation of images as passwords. Human brain is good in remembering picture than textual character. There are various graphical password schemes or graphical password software in the market. However, very little research has been done to analyse graphical passwords that are still immature. There for, this project work merges persuasive cued click points and password guessing resistant protocol. The major goal of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess. Well known security threats like brute force attacks and dictionary attacks can be successfully abolished using this method.

Key words: CaRP, CbPA, CPA, User Authentication, Security, PCCPs

I. INTRODUCTION

People select predictable passwords. This occurs with both text based and graphical passwords. Users tend choose passwords to that are memorable in some way, which unfortunately often means that the passwords tend to follow predictable patterns that are easier for attackers to exploit. 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. An authentication system should encourage strong passwords while still maintaining memorability. People select predictable passwords. This occurs with both text based and graphical passwords. Users tend choose passwords to that are memorable in some way, which unfortunately often means that the passwords tend to follow predictable patterns that are easier for attackers to exploit. 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. An authentication system should encourage strong passwords while still maintaining memorability. Authentication determines whether a user should be allowed access to a particular system or resource. Using hard AI (Artificial Intelligence) problems for security 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 beyond the capability of computers but easy for humans. Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots. However, this new paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications. We introduce new security primitive based on hard AI problems, namely, a novel family of graphical password systems integrating Captcha technology, which we call CaRP (Captcha as gRaphical Passwords). CaRP is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. Unlike other click-based graphical passwords, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every login attempt.The notion of CaRP is simple but generic. CaRP can have multiple instantiations. In theory, any Captcha scheme relying on multiple-object classification can be converted to a CaRP scheme. 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. Intuitive countermeasures such as throttling logon attempts do not work well for two reasons:

1) It causes denial-of-service attacks and incurs expensive helpdesk costs for account reactivation.
2) It is vulnerable to global password attacks whereby adversaries intend to break into any account rather than a specific one, and thus try each password candidate on multiple accounts and ensure that the number of trials on each account is below the threshold to avoid triggering account lockout.CaRP also offers protection against relay attacks, an increasing threat to bypass Captchas protection, wherein Captcha challenges are relayed to humans to solve. Koobface was a relay attack to bypass Facebook's Captcha in creating new accounts. CaRP is robust to shoulder-surfing attacks if combined with dual-view technologies.

II. RELATED WORKS

First time CAPTCHA was invented in 2000 at Carnegie Mellon University by John Langford, Nicholas J. Hooper and Luis Von Ahn . CAPTCHA is an acronym for "Completely Automated Public Turning Test to tell Computers and Humans Apart" . The progress of Internet, Web security has become an important issue. There are too many malicious threats across the Internet which may compromise your system in the absence of any secure application which provides protection against such threats. One such threat is the Bot. A Bot is a malicious program which has the capability to run automated tasks over the network and thus creating problem in the network .

CAPTCHA is one such shield which can be used as a protection from these malicious programs like Bot.

A. Categories of CAPTCHA:

CAPTHCAs means presenting a challenge response test to the users or humans. They are classified based on what is distorted that is whether characters, digits, or images. Some types of CAPTCHAs are given below:

- CAPTCHAs based on text.
- CAPTCHAs based on image.
- CAPTCHAs based on audio.

1) CAPTCHAs based on text: Text based CAPTCHAs is a very simple to implement. It is very effective and requires a large question bank. In Text based captcha the Number of classes of characters and digits are very small so the problem occurs for user to identify the correct characters and digits. The text based captcha is possible to identify the character and digit through Optical character recognition (OCR) technique. In Text based CAPTCHAs simple asked questions like as based on arithmetic equation some example are given below:

- What is three plus two (3+2=?).
- What is six minus one (6-1=?).
- Which of cabbage, apple and table is vegetable?

Fig. 1: Text based Graphical password

2) CAPTCHAs based on image: Graphics-based CAPTCHAs are challenge-tests in which the users have to guess those images that have some similarity. For example: visual puzzles. In image based CAPTCHAs user is required to identity image. The advantage of image based. CAPTCHA is that pattern recognition is hard AI problem and therefore it is difficult to break this test using pattern recognition technique. Example of images based CAPTCHA are given below

Fig. 2: Image based graphical Password.

3) CAPTCH As based on audio: Audio-based CAPTCHAs are based on the sound-based systems. These CAPTCHAs are developed for visually disabled users. It contains downloadable audio-clips. In this type of CAPTCHA, first the user listens and after that submits the spoken word . The first sound-based system name ECO was implemented by the Nancy Chan a student from the City University in Hong Kong. The audio-based system is based on the difference in the ability between computer machines and humans in recognizing spoken language. The program chooses a sequence of digits and words randomly and renders the words and number digits into sound clips and distorts it. The distorted sound clip is then presented to the user to enter the right word or number. The user is asked to enter exactly the same words as spoken the audio clip.

Example of audio based CAPTCHA are given below.

Fig. 3: audio as a graphical password

III. 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 withdual-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. Defence against online dictionary attacks is a more subtle problem than it might appear.

IV. SYSTEM ARCHITECTURE

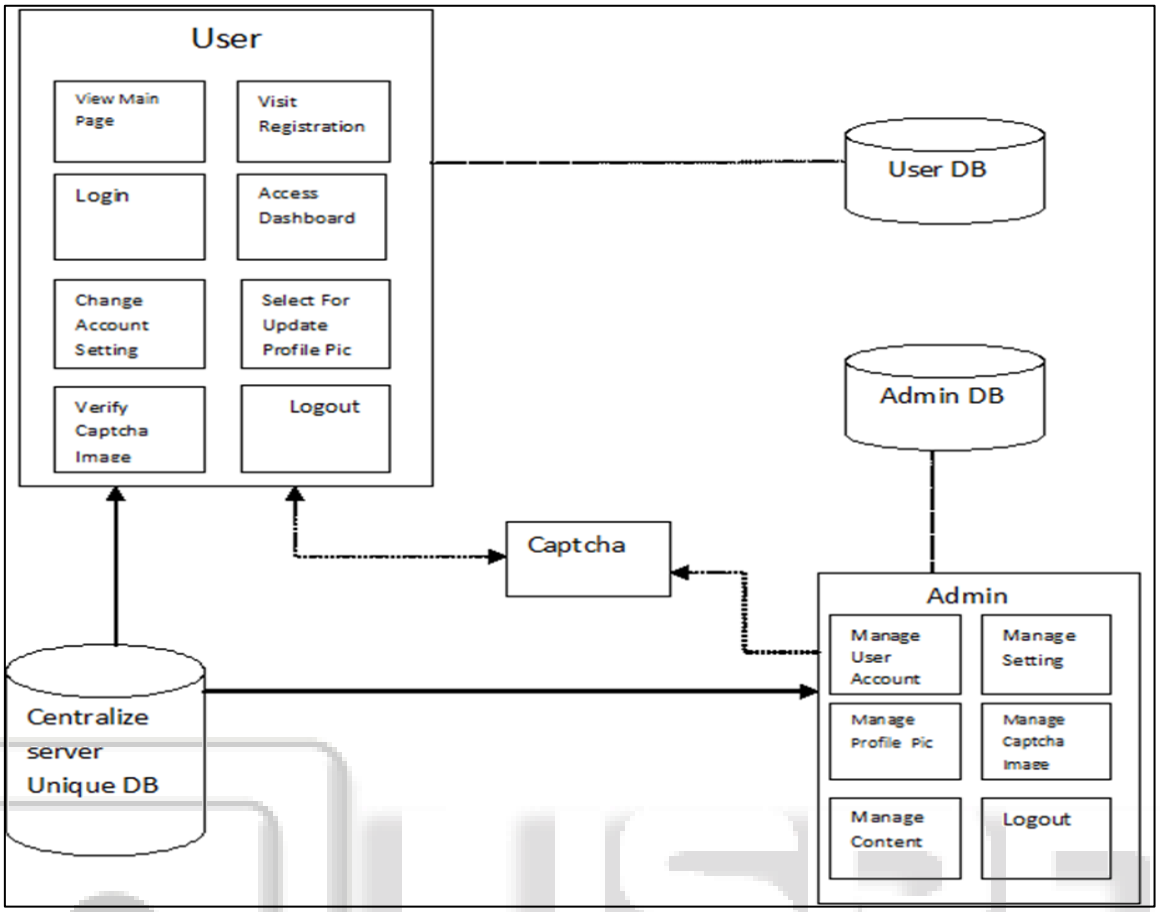

Fig. 4: System Architecture

V. ADVANTAGE OF PROPOSED SYSTEM

It offers reasonable security and usability and appears to fit well with some practical applications for improving online security. 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.

VI. APPLICATION

1) *Authenticating the User:*
   - System
   - Applications
2) *Locking/Unlocking:*
   - Hard Disk
   - Folders
   - Files

VII. CONCLUSION

The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. In this paper, we have 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. Our preliminary analysis suggests that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware. However, since there is not yet wide deployment of graphical password systems, the vulnerabilities of graphical passwords are still not fully understood.Overall, the current graphical password techniques are still immature. Much more research and user studies are needed for graphical password techniques to achieve higher levels of maturity and usefulness.

REFERENCES

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys, vol. 44, no. 4, 2012.
[2] (2012, Feb.). The Science Behind Passfaces [Online]. Available:http://www.realuser.com/published/ScienceBehindPassfaces.pdf
[3] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proc. 8th USENIX Security Symp., 1999, pp. 1–15.
[4] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292, 2008.
[5] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and

longitudinal evaluation of a graphical password system," Int. J. HCI, vol. 63, pp. 102–127, Jul. 2005.
[6] P. C. van Oorschot and J. Thorpe, "On predictive models and user- drawn graphical passwords," ACM Trans. Inf. Syst. Security, vol. 10, no. 4, pp. 1–33, 2008.
[7] K. Golofit, "Click passwords under investigation," in Proc. ESORICS, 2007, pp. 343–358.
[8] A. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in Proc. Symp. Usable Privacy Security, 2007, pp. 20–28.
[9] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot spots in graphical passwords," in Proc. USENIX Security, 2007, pp. 103–118.
[10] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on passpoints-style graphical passwords," IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 393–405, Sep. 2010.

