

Full Length Article

Captcha: Visual Passwords For Robust Authentication Through Difficult AI Tasks

Vaishnav Mathurdas¹, Mr.Bhuvan²

B.Tech Student, Department Of Electronics and Computer Engineering, J.B Institute of Engineering and Technology, Hyderabad, India¹

Assistant Professor, Department Of Electronics and Computer Engineering, J.B Institute of Engineering and Technology, Hyderabad, India²

Mathurdasvaishnav123@gmail.com, bhuvan.ecm@jbiet.edu.in

Article Received 22-12-2025, Revised 15-01-2026, Accepted 22-01-2026

Authors Retains the Copyrights of This Article

Abstract

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 under-explored. In this project, 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 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.

Keyword: CaRP, AI.

Introduction

What is Secure Computing?

Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural

disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.



Fig:1.1: Secure computing

Working conditions and basic needs in the secure computing:

If you don't take basic steps to protect your work computer, you put it and all the information on it at risk. You can potentially compromise the operation of other computers on your organization's network, or even the functioning of the network as a whole.

1. Physical security:

Technical measures like login passwords, anti-virus are essential. (More about those below) However, a secure physical space is the first and more important line of defense.

Is the place you keep your workplace computer secure enough to prevent theft or access to it while you are away?

While the Security Department provides coverage across the Medical center, it only takes seconds to steal a computer, particularly a portable device like a laptop or a PDA.

A computer should be secured like any other valuable possession when you are not present.

2. Access passwords:

The University's networks and shared information systems are protected in part by login credentials (user-IDs and passwords). Access passwords are also an essential protection for personal computers in most circumstances. Offices are usually open and shared spaces, so physical access to computers cannot be completely controlled.

To protect your computer, you should consider setting passwords for particularly sensitive applications resident on the computer (e.g., data analysis software), if the software provides that capability.

3. Prying eye protection:

Because we deal with all facets of clinical, research, educational and administrative data here on the medical campus, it is important to do everything possible to minimize exposure of data to unauthorized individuals.

4. Anti-virus software:

Up-to-date, properly configured anti-virus software is essential. While we have server-side anti-virus software on our network computers, you still need it on the client side (your computer).

5. Firewalls:

Anti-virus products inspect files on your computer and in email. Firewall software and hardware monitor communications between your computer and the outside world. That is essential for any networked

computer.

6. Software updates:

It is critical to keep software up to date, especially the operating system, versions will contain fixes for discovered vulnerabilities.

Almost all anti-virus have automatic update features (including

SAV). Keeping the "signatures" (digital patterns) of malicious software detectors up-to-date is essential for these products to be effective.

7. Keep secure backups:

Even if you take all these security steps, bad things can still happen. Be prepared for the worst by making backup copies of critical data, and keeping those backup copies in a separate, secure location. For example, use supplemental hard drives, CDs/DVDs, or flash drives to store critical, hard-to-replace data.

8. Report problems:

If you believe that your computer or any data on it has been compromised, you should make a information security incident report. That is required by University policy for all data on our systems, and legally required for health, education, financial and any other kind of record containing identifiable personal information.

Literature Survey

1. On predictive models and user drawn graphical passwords AUTHORS: P. C. van Oorschot and J. Thorpe

In commonplace 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 (e.g., graphical) are also vulnerable to dictionary attack because of users tending to choose memorable

passwords. We suggest a method to predict and model a number of such classes for systems where passwords are created solely from a user's memory. We hypothesize that these classes define weak password subspaces suitable for an attack dictionary. For user-drawn graphical passwords, we apply this method with cognitive studies on visual recall.

These cognitive studies motivate us to define a set of password complexity factors (e.g., reflective symmetry and stroke count), which define a set of classes. To better understand the size of these classes and, thus, how weak

the password subspaces they define might be, we use the “Draw-A-Secret” (DAS) graphical password scheme of Jermyn et al. [1999] as an example. We analyze the size of these classes for DAS under convenient parameter choices and show that they can be combined to define apparently popular subspaces that have bit sizes ranging from 31 to 41—a surprisingly small proportion of the full password space (58 bits).

Our results quantitatively support suggestions that user-drawn graphical password systems employ measures, such as graphical password rules or guidelines and proactive password checking.

2. Modeling user choice in the Pass Points graphical password scheme

AUTHORS: A. E. Dirik, N. Memon, and J.-C. Birget
 We develop a model to identify the most likely regions for users to click in order to create graphical passwords in the Pass Points system. A PassPoints password is a sequence of points, chosen by a user in an image that is displayed on the screen. Our 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 allows us to evaluate automatically whether a given image is well suited for the PassPoints system, and to analyze possible dictionary attacks against the system. We compare the predictions provided by our model to results of experiments involving human users. At this stage, our 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.

Project Design

Input Design

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.

- Methods for preparing input validations and steps to follow when error occur.

Objectives

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system’s relationship to help user decision-making. 1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements. 2. Select methods for presenting information.

Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

System Architecture

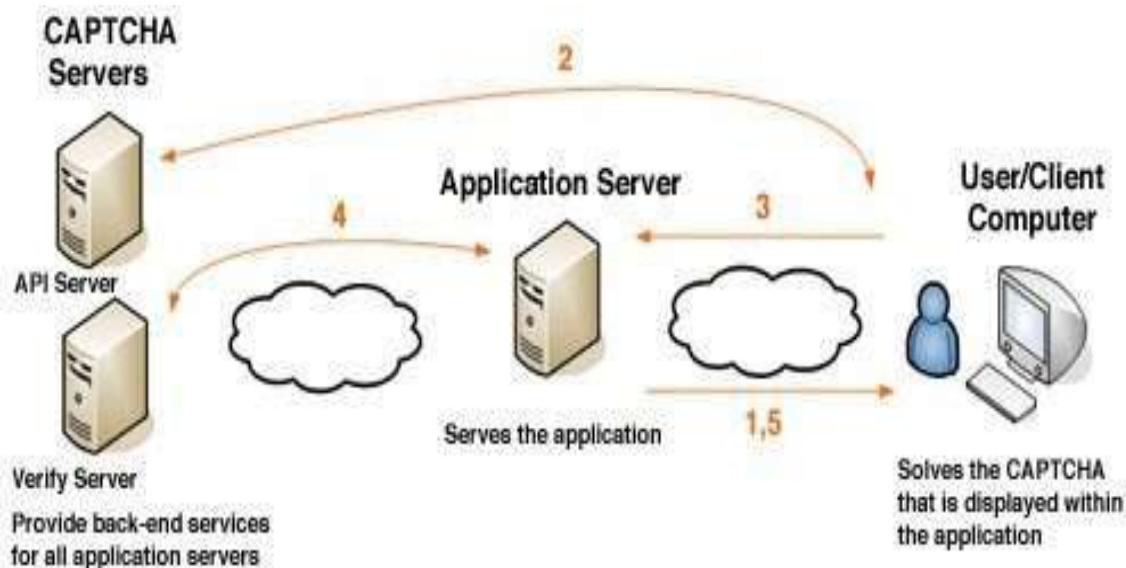


Fig:3.3: System Architecture

Results

User Registration:



Fig:1: User Registration

Admin Login:



Fig:2: Admin Login

Admin Activating User:



Fig:3: Admin Activating User

User Login (Enter User Name):



Fig:5.4: User Login

User Login (Enter Password & Captcha Code):

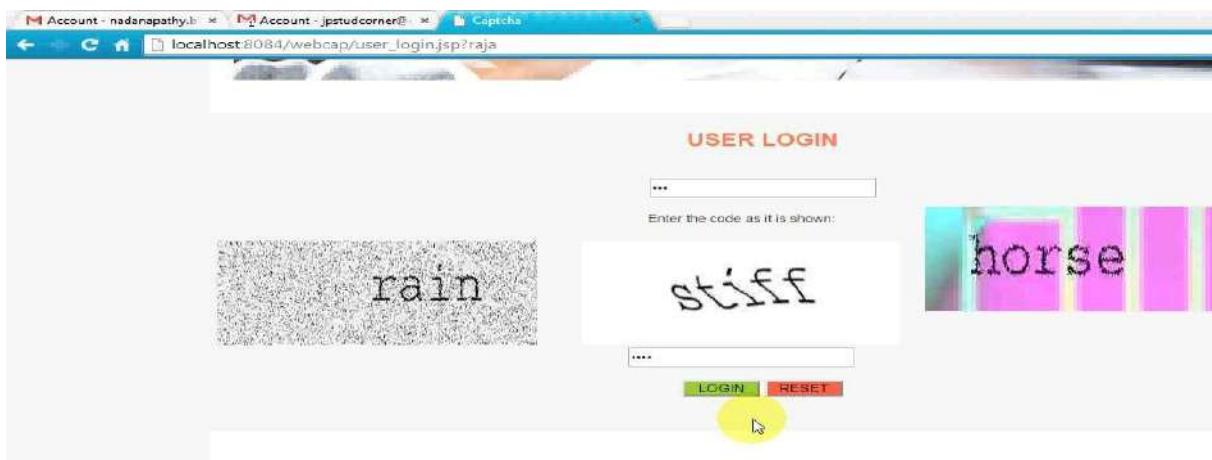


Fig:4: User Login

User Upload (Click Image & Upload):



Fig:5: User Upload

User Download:



Fig:6: User Download

User Download (Click Image & Download):



Fig:6: User Download



Fig:7: If User Click Invalid Coordinates

When you click correct coordinates:



Fig:8: If User Click Correct Coordinates

File Downloading:



Fig:9: File Downloading

Viewing Downloaded File:

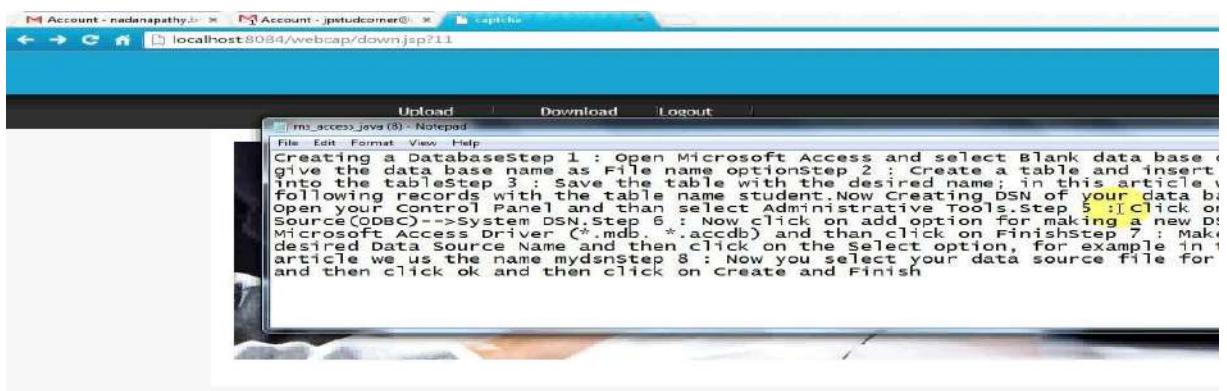


Fig:10: Viewing Downloaded File

When user login If he entered invalid captcha code means your account will be blocked and alert will come to your registered mail.

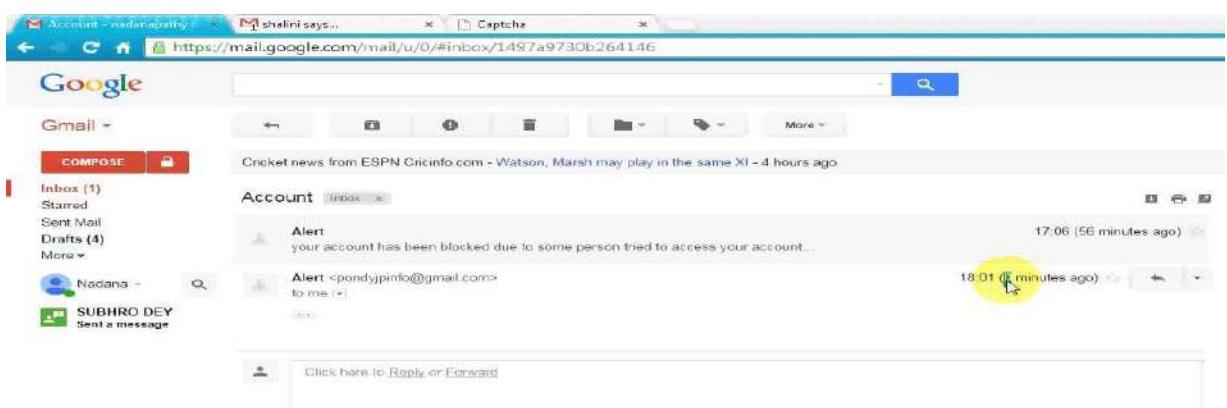


Fig:11: Account Block & Alert

Admin Activating Blocked user:



Fig:12: Admin Activating

Conclusion

In this Project We have proposed CaRP, a new security primitive relying on unsolved hard AI problems. CaRP is both a Captcha and a graphical password scheme. 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. Hotspots in CaRP images can no longer be exploited to mount automatic online guessing attacks, an inherent vulnerability in many graphical password systems. CaRP forces adversaries to resort to significantly less efficient and much more costly human-based attacks. In addition to offering protection from online guessing attacks, CaRP is also resistant to Captcha relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. CaRP can also help reduce spam emails sent from a Web email service.

Our usability study of two CaRP schemes we have implemented is encouraging. For example, more participants considered AnimalGrid and ClickText easier to use than PassPoints and a combination of text password and Captcha. Both AnimalGrid and ClickText had better password memorability than the conventional text passwords. On the other hand, 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. The optimal tradeoff between security and usability remains an open question for CaRP, and further studies are needed to refine CaRP for actual deployments.

Like Captcha, CaRP utilizes unsolved AI problems. However, a password is much more valuable to attackers than a free email account that Captcha is typically used to protect. Therefore there are more incentives for attackers to hack CaRP than Captcha. That is, more efforts will be attracted to the following win-win game by CaRP than ordinary Captcha: If attackers succeed, they contribute to improving AI by providing solutions to open problems such as segmenting 2D texts. Otherwise, our system stays secure, contributing to practical security. 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. Overall, our work is one step forward in the paradigm of using hard AI problems for security. Of reasonable security and usability and practical applications, CaRP has good potential for refinements, which call for useful future work. More importantly, we expect CaRP to inspire new inventions of such AI based security primitives.

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. Monroe, 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 userdrawn 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.

[11] P. C. van Oorschot and J. Thorpe, “Exploiting predictability in clickbased graphical passwords,” J. Comput. Security, vol. 19, no. 4, pp. 669–702, 2011.

[12] T. Wolverton. (2002, Mar. 26). Hackers Attack eBay Accounts [Online]. Available: <http://www.zdnet.co.uk/news/networking/2002/03/26/hack>

[ers-attack-ebay-accounts-2107350/](http://www.zdnet.co.uk/news/networking/2002/03/26/hack)

[13] HP TippingPoint DVLabs, Vienna, Austria. (2010). Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs [Online]. Available: <http://dvlabs.tippingpoint.com/toprisks2010>

[14] B. Pinkas and T. Sander, “Securing passwords against dictionary attacks,” in Proc. ACM CCS, 2002, pp. 161–170.

[15] P. C. van Oorschot and S. Stubblebine, “On countering online dictionary attacks with login histories and humans-in-the-loop,” ACM Trans. Inf. Syst. Security, vol. 9, no. 3, pp. 235–258, 2006.

[16] M. Alsaleh, M. Mannan, and P. C. van Oorschot, “Revisiting defenses against large-scale online password guessing attacks,” IEEE Trans. Dependable Secure Comput., vol. 9, no. 1, pp. 128–141, Jan./Feb. 2012.

[17] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, “CAPTCHA: Using hard AI problems for security,” in Proc. Eurocrypt, 2003, pp. 294–311.

[18] S. Chiasson, P. C. van Oorschot, and R. Biddle, “Graphical password authentication using cued clickpoints,” in Proc. ESORICS, 2007, pp. 359–374.

[19] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, “Influencing users towards better passwords: Persuasive cued click-points,” in Proc. Brit. HCI Group Annu. Conf. People Comput., Culture, Creativity, Interaction, vol. 1, 2008, pp. 121–130.

[20] D. Davis, F. Monrose, and M. Reiter, “On user choice in graphical password schemes,” in Proc. USENIX Security, 2004, pp. 1–11.

[21] R. Dhamija and A. Perrig, “Déjà Vu: A user study using images for authentication,” in Proc. 9th USENIX Security, 2000, pp. 1–4.

[22] D. Weinshall, “Cognitive authentication schemes safe against spyware,” in Proc. IEEE Symp. Security Privacy, May 2006, pp. 300–306.

[23] P. Dunphy and J. Yan, “Do background images improve ‘Draw a Secret’ graphical passwords,” in Proc. ACM CCS, 2007, pp. 1–12.

[24] P. Golle, “Machine learning attacks against the Asirra CAPTCHA,” in Proc. ACM CCS, 2008, pp. 535–542.