Captcha as Graphical Passwords-A New Security Primitive Based On Hard AI Problems

Mrs. G. Rajani[*1], Dr. P. Praveen Kumar[*2]
[1]MCA Student, Department of Master of Computer Applications,
Vignan's Institute of Information Technology(A), Beside VSEZ,Duvvada,Vadlapudi Post, Gajuwaka, Visakhapatnam-530049.
[2]Assistant Professor, Department of Information Technology,
Vignan's Institute of Information Technology(A), Beside VSEZ,Duvvada,Vadlapudi Post, Gajuwaka, Visakhapatnam-530049.
vignaniit.edu.in

Abstract:

Many security primitives are based on hard mathematical problems. A promising new paradigm that hasn't received much attention yet is hard AI problems for security. In this paper, Captcha as graphical passwords (CaRP), a unique family of graphical password systems built on top of Captcha technology. This security primitive is based on challenging AI problems. CaRP is a password system using graphics and a captcha. CaRP can prevent shoulder-surfing assaults as well as online guessing attacks and relay attacks when used in conjunction with dual-view technology. Notably, even if the password is in the search set, a CaRP password can only be retrieved probabilistically by automated online guessing assaults. Also addressed by CaRP is the well-known picture hotspot issue, which frequently results in the use of weak passwords in popular graphical password systems like PassPoints. 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.

Keywords: Captcha,Graphical Passwords,Online Security,Artificial Intelligence,Mathematical Problems.

1. INTRODUCTION

Your description of computer security is accurate. It encompasses a broad range of measures and practices aimed at protecting computer systems, networks, and data from various threats, whether they are intentional (e.g., hacking or cyber attacks) or unintentional (e.g., system failures or natural disasters). Here are some key points related to computer security:

1. Access Control: Limiting access to authorized users and ensuring that only those with the appropriate permissions can access specific resources.

2. Data Encryption:The process of converting data into a secure format (cipher text) to prevent unauthorized access. It ensures that even if data is intercepted, it remains unreadable without the decryption key.

3. Passwords: Using passwords as a form of authentication to verify the identity of users before granting access to a system, application, or data.

4. Firewalls: Implementing firewalls to monitor and control incoming and outgoing network traffic, acting as a barrier between a trusted internal network and untrusted external networks, such as the internet.

5. Antivirus Software: Employing antivirus programs to detect, prevent, and remove malicious software (malware) such as viruses, worms, and trojan horses.

6. Intrusion Detection and Prevention Systems (IDPS):Monitoring network and/or system activities for malicious activities or security policy violations and taking preventive measures.

7. Security Policies: Establishing and enforcing policies that define acceptable use, password requirements, data handling procedures, and other security-related guidelines within an organization.

8. Regular Software Updates: Keeping software, operating systems, and applications up-to-date with the latest security patches to address vulnerabilities and bugs.

9. Physical Security: Protecting physical access to computers, servers, and networking equipment to prevent unauthorized individuals from physically tampering with or stealing hardware.

10. Backup and Disaster Recovery: Creating regular backups of critical data and implementing disaster recovery plans to ensure business continuity in the event of data loss or system failures.

11. Security Awareness Training:Educating users about security best practices, potential threats, and the importance of adhering to security policies.

12. Incident Response Planning: Developing plans and procedures to effectively respond to and recover from security incidents, minimizing the impact on the organization.

As technology evolves, so do the challenges and threats to computer security. Therefore, staying informed about the latest developments in cybersecurity and adopting a proactive approach to security is crucial for organizations and individuals alike.

2. LITERATURE SURVEY

The most important step in the software development process is the literature review. This will describe some preliminary research that was carried out by several authors on this appropriate work and we are going to take some important articles into consideration and further extend our work.The literature review you provided offers a comprehensive overview of existing research and advancements in the field of integrating ChatGPT with itself. The identified papers cover a range of topics, from the foundational introduction of ChatGPT to its potential integration with reinforcement learning, transfer learning, and dialogue systems. Here's a summary of the key points: The literature survey you provided seems to focus on the vulnerabilities associated with text-based and graphical password schemes, exploring the likelihood of users choosing easily predictable or memorable passwords. Below is a detailed breakdown of the key points discussed in the text:

1. Introduction to Password Vulnerabilities:

- Common text-based password schemes are susceptible to users selecting easily recallable and patterned passwords, making them vulnerable to brute-force dictionary attacks.
- The concern arises whether different password types, including graphical passwords, are also prone to dictionary attacks due to users' tendencies to choose memorable options.

2. Previous Work by P. C. van Oorshot et al.:

- P. C. van Oorshot et al. propose a method to predict and model various password classes, especially in systems where passwords are solely created from a user's memory.
- The method aims to identify weak password subspaces that can be exploited in dictionary attacks.

3. Hypothesis and Cognitive Studies on Visual Recall:

- The authors hypothesize that these identified classes represent weak password subspaces suitable for dictionary attacks.
- For user-drawn graphical passwords, the method is applied, incorporating cognitive studies on visual recall to enhance the understanding of user behavior.

4. Password Complexity Factors for Graphical Passwords:

- Cognitive studies inform the definition of a set of password complexity factors for graphical passwords, including features like reflective symmetry and stroke count.
- These factors contribute to the creation of distinct classes within the graphical password space.

5. Application to "Draw-A-Secret" (DAS) Graphical Password Scheme:

- The study employs the "Draw-A-Secret" (DAS) graphical password scheme as an example to analyze the size of identified password classes.
- The analysis is conducted under convenient parameter choices to understand the weaknesses in password subspaces.

6. Quantitative Results:

- The results indicate that the classes identified in DAS can be combined to define apparently popular subspaces with bit sizes ranging from 31 to 41.
- This represents a surprisingly small proportion of the full password space (58 bits), highlighting potential vulnerabilities in the graphical password scheme.

7. Implications and Recommendations:

- The findings support suggestions that user-drawn graphical password systems need additional measures, such as graphical password rules, guidelines, and proactive password checking.
- There is a need for modeling user choice in graphical password schemes to enhance security.

In summary, the literature survey provides a comprehensive exploration of the vulnerabilities in both text-based and graphical password schemes, emphasizing the importance of understanding user behavior and implementing additional measures to mitigate potential security risks.

3. EXISTING SYSTEM

Captcha, an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart," is a widely adopted security measure on the internet. It is designed to differentiate between human users and automated computer programs (bots) by presenting challenges that are easy for humans to solve but difficult for computers. Captcha is commonly used to protect online email accounts, website registrations, and other online services from abuse by automated bots.

Limitations and Problems in the Existing System:

1. Limited Success Against Advanced Bots:
- While Captcha has been effective in preventing automated attacks from basic bots, it has faced challenges in dealing with more advanced bots equipped with sophisticated algorithms and machine learning capabilities.

2. Usability Concerns:
- Captcha challenges, especially those involving distorted characters or complex visual puzzles, can be frustrating for users. The usability issues can lead to a poor user experience, causing inconvenience and potential drop-offs.

3. Accessibility Challenges:
- Captcha challenges based on visual or auditory elements can be problematic for users with visual or hearing impairments, limiting the accessibility of certain online services for a portion of the population.

4. Innovation in Automated Solving Techniques:
- Over time, automated methods for solving Captcha challenges have evolved. There are now sophisticated tools and services that use advanced image recognition, machine learning, or even human workers to bypass traditional Captcha systems, reducing their effectiveness.

5. Resource Intensive:
- Some Captcha implementations, particularly those involving complex puzzles or interactive tasks, can be resource-intensive, causing delays in the user authentication process and potentially affecting website performance.

6. Lack of Universality:
- Captcha systems vary across websites, leading to a lack of standardization. Users are often required to adapt to different Captcha mechanisms on different platforms, contributing to a fragmented user experience.

7. Security Risks of Over-reliance:
- Depending solely on Captcha for security may create a false sense of security. Over-reliance on this single mechanism may lead to neglect of other security measures, leaving systems vulnerable to other forms of attacks.

8. Constant Evolution of Automated Attacks:
- As technology advances, so do the capabilities of automated bots. Captcha, being a static defense mechanism, struggles to keep up with the continuous evolution of techniques employed by malicious actors to bypass security measures.

In conclusion, while Captcha has been a significant advancement in distinguishing between humans and bots, its limitations, including usability concerns, accessibility issues, and susceptibility to evolving automated attacks, highlight the need for ongoing innovation in internet security mechanisms. There is a continuous challenge

to strike a balance between security and user experience in the ever-changing landscape of online threats.

4. PROPOSED SYSTEM

The proposed system, Captcha as Graphical Passwords (CaRP), introduces a novel security primitive that combines the concept of Captcha with graphical password systems. CaRP aims to address multiple security challenges, including online guessing attacks, relay assaults, and shoulder-surfing attacks when utilized in conjunction with dual-view technology.

Advantages of CaRP:

1. Enhanced Security against Online Guessing Attacks: CaRP strengthens security by introducing AI-driven graphical challenges, making it more resilient against automated online guessing attacks. The integration of challenging AI problems enhances the complexity of authentication, making it harder for malicious actors to gain unauthorized access.

2. Protection from Relay Attacks: Relay attacks involve intercepting and manipulating communication between the user and the system. CaRP offers protection against relay attacks, a growing threat in the context of compromising traditional Captcha security. The system introduces measures to thwart attempts to exploit vulnerabilities in the communication channel.

3. Defense against Shoulder-Surfing Attacks: CaRP, when used in conjunction with dual-view technology, mitigates the risk of shoulder-surfing attacks. Dual-view technology involves presenting different views or perspectives of graphical challenges to the user, making it more challenging for an onlooker to decipher the authentication information.

4. Resistance to Password Dictionary Attacks: CaRP provides a defense mechanism against password dictionary attacks, which have historically been a significant security risk for various online services. The graphical password system adds an additional layer of complexity beyond traditional text-based passwords, making it more challenging for attackers to exploit known password lists.

5. Incorporation of AI-driven Challenges: The incorporation of challenging AI problems adds an element of unpredictability and adaptability to the authentication process. This not only enhances security but also allows for continuous evolution to counter emerging threats and attack techniques.

6. User-Friendly Graphical Password System: CaRP maintains the user-friendly aspect of graphical password systems by presenting challenges in a visually intuitive manner. This ensures a positive user experience while maintaining a high level of security.

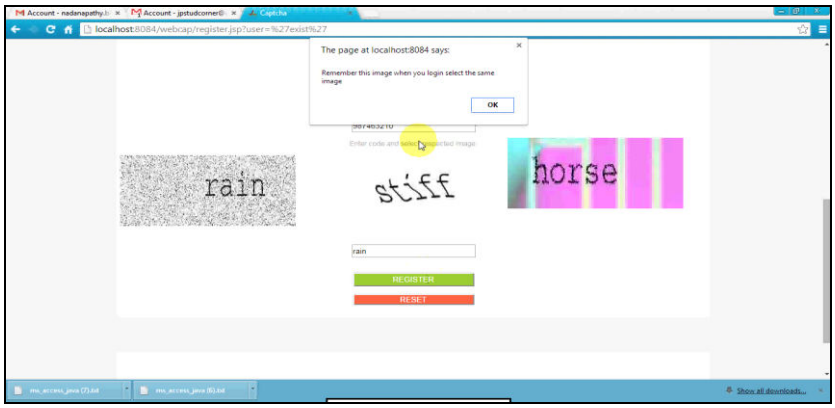
7. Potential for Customization and Variety: The CaRP system offers the potential for customization and variety in graphical challenges, reducing the predictability of authentication methods. This adaptability adds an extra layer of security against attackers attempting to exploit repetitive patterns.

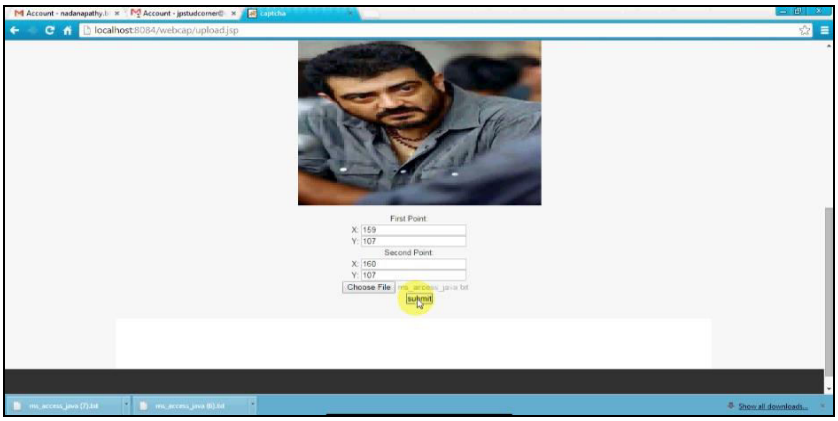
8. Compliance with Industry Security Standards: - By addressing multiple security challenges, including those associated with relay attacks and online guessing, CaRP aligns with industry security standards and best practices, providing a robust solution for online service protection.

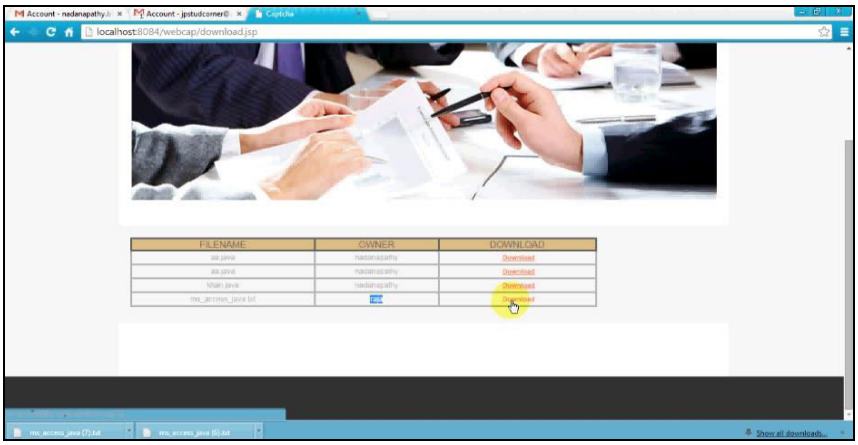
5. EXPERIMENTAL RESULTS

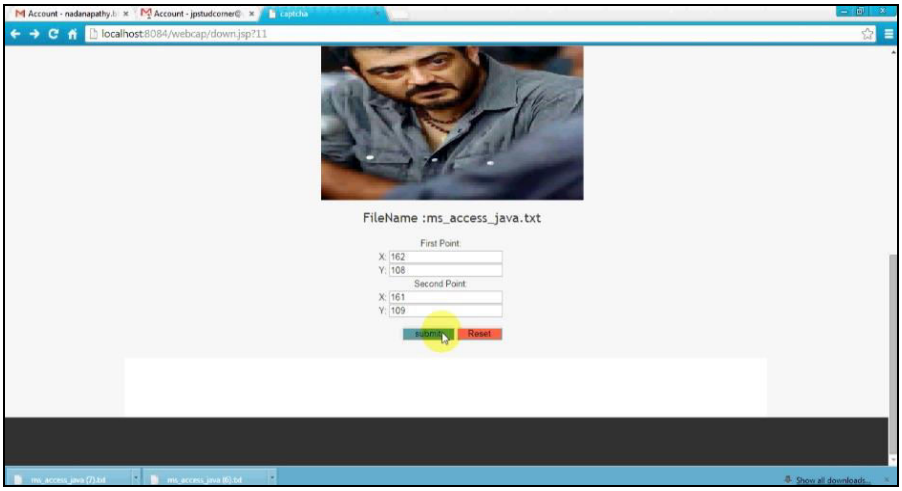
From the below figures it can be seen that proposed model is more accurate in order to prove our proposed system.

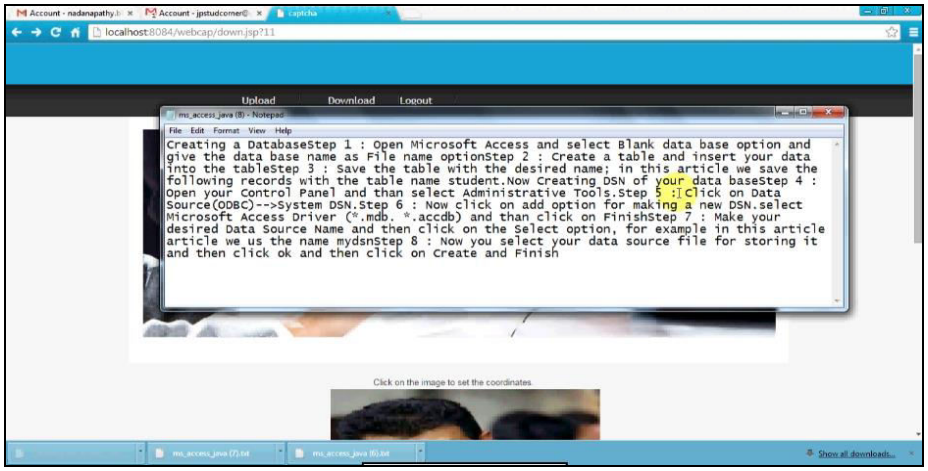
Main Window

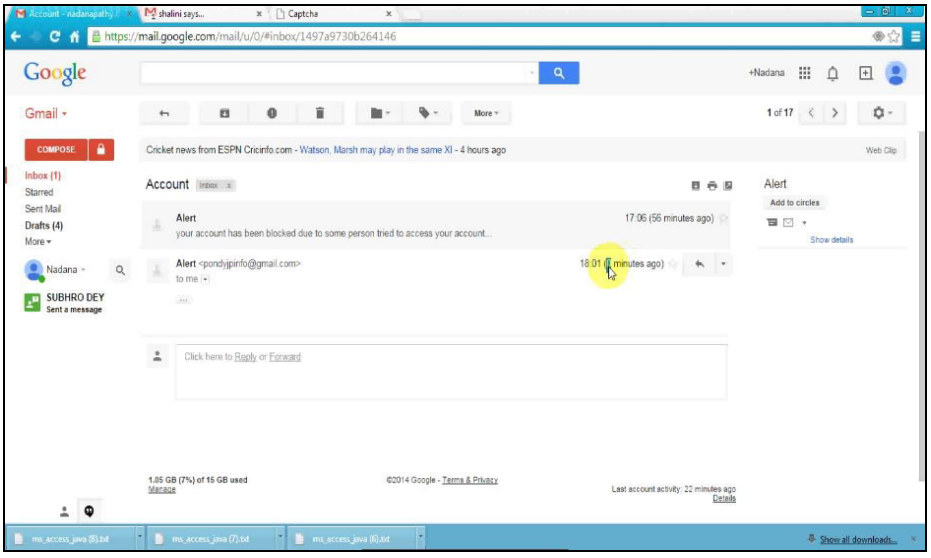







localhost:8084/webcap/down.jsp?11
FileName :ms_access_java.txt
First Point
X: 162
Y: 108
Second Point
X: 161
Y: 109
submit
Reset


localhost:8084/webcap/down.jsp?11
Upload
Download
Logout
Creating a DatabaseStep 1 : Open Microsoft Access and select Blank data base option and give the data base name as File name optionStep 2 : Create a table and insert your data into the tableStep 3 : Save the table with the desired name; in this article we save the following records with the table name student.Now Creating DSN of your data baseStep 4 : Open your Control Panel and than select Administrative Tools.Step 5 : Click on Data Source(ODBC)-->System DSN.Step 6 : Now click on add option for making a new DSN.select Microsoft Access Driver (*.mdb, *.accdb) and than click on FinishStep 7 : Make your desired Data Source Name and then click on the Select option, for example in this article article we us the name mydsnStep 8 : Now you select your data source file for storing it and then click ok and then click on Create and Finish
Click on the image to set the coordinates


https://mail.google.com/mail/u/0/#inbox/1497a9730b264146
Google
Gmail
COMPOSE
Inbox (1)
Starred
Sent Mail
Drafts (4)
More
Account
Alert
your account has been blocked due to some person tried to access your account...
Alert <pondyjpinfo@gmail.com>
to me
Click here to Reply or Forward
SUBHRO DEY
Sent a message

6. CONCLUSION

CaRP is a cutting-edge security innovation rooted in unresolved AI challenges. It functions as a captcha-enabled graphical password system where each login attempt involves a unique CaRP image, serving as both a graphical password and a captcha challenge. This innovative approach ensures that online guessing attacks remain computationally independent, enhancing security. CaRP's standout feature is its probabilistic password retrieval, making automated guessing attempts, including brute-force attacks, highly challenging. Notably, CaRP mitigates common graphical password vulnerabilities, thwarting automated attacks and encouraging costlier, less successful human-based efforts. Usability studies indicate positive feedback, with participants finding it easier to use than traditional methods, and it offers better password memorability. Future enhancements are envisioned, particularly in balancing security and usability. Moreover, CaRP's potential extends to the realm of AI-based security, motivating further research in this evolving field. Its adaptability ensures ongoing security in the face of emerging threats, making it a catalyst for the development of advanced AI-based security systems.

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 userdrawn graphical passwords," *ACM Trans. Inf. Syst. Security*, vol. 10, no. 4, pp. 1–33, 2008.