Captcha as Graphical Passwords—a New Security Primitive Based on Hard AI Problems

1M.Ramapriya, 2R.Yamini, 3Mr.M.KrishnaMoorthy
1,2PG Scholar, 3 Assistant Professor,
Department of MCA, Panimalar Engineering College

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. A novel family of graphical password systems built on top of Captcha technology, which we call Captcha as a graphical passwords (CaRP). CaRP addresses such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. 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 solution, but it offers logical security and usability and appears to fit well with some practical applications for improving accessible security.

1. INTRODUCTION

A FUNDAMENTAL task in security is to create cryptographic primitives based on hard problems that are computationally difficult. For example, the problem of numeral factorization is fundamental to the RSA public-key cryptosystem. The discrete logarithm problem is fundamental to the ElGamal encryption, the Diffie-Hellman key exchange, the Digital Signature Algorithm, the elliptic curve cryptography and so on.

The most notable primitive invented is Captcha, which distinguishes from users to computers by presenting a challenge, i.e., a puzzle Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots. CaRP is click-based graphical passwords, where a series of snaps on an image is used to derive a password.

II. BACKGROUND AND RELATED WORK

A. Graphical Passwords:

- A huge number of graphical password schemes have been suggested. They can be classified into three categories according to the task involved in learning and entering passwords: recognition, remembrance, and indicated recall.
- A recognition-based scheme requires identifying among decoys the visual objects belonging to a password portfolio. A remembrance-based scheme requires a user to regenerate the same interaction result without cueing. Draw-A-Secret (DAS) was the first recall-based scheme proposed. In an Indicted-recall scheme, an external cue is provided to help and bots in solving certain hard AI problems.

B. Captcha

Captcha relies on the gap of expertise between users and bots in solving certain hard AI problems. There are two types of visual Captcha: transcript Captcha and Image-Recognition Captcha (IRC). Transcript Captcha should rely on the difficulty of character segmentation, which is computationally expensive and combinatorially hard memorize and enter a password.
segmentation, which is computationally expensive and combinatorially hard.

C. Captcha in Authentication

It was introduced in to use both Captcha and password in a user authentication protocol, which we call Captcha-based Password Authentication (CbPA) protocol, to counter real time dictionary attacks.

III. CAPTCHA AS GRAPHICAL PASSWORDS

A. New Way to Thwart Guessing Attacks

In a guessing attack, a password guess tested in an unsuccessful trial is established wrong and excluded from succeeding trials. Mathematically, let $S$ be the set of password guesses before any trial, $\rho$ be the password to find, $T$ denote a trial whereas $Tn$ denote the $n$-th trial, and $p(T = \rho)$ be the probability that $\rho$ is tested in trial $T$. Let $En$ be the set of password guesses tested in trials up to (including) $Tn$. The password guess to be tested in $n$-th trial $Tn$ is from set $S\setminus En-1$, i.e., the relative complement of $En-1$ in $S$.

B. CaRP: An Overview

In CaRP, a new image is generated for every login challenge, even for the same user. CaRP uses an alphabet of visual objects e.g. alphanumerical characters, similar animals) to generate a CaRP image, which is also a Captcha task.

C. Converting Captcha to CaRP

In principle, any visual Captcha scheme depend on recognizing two or more predefined types of objects can be converted to a CaRP. All text Captcha structures and most IRCs meet this requirement.

D. User Authentication With CaRP Schemes

Assume that CaRP schemes are used with additional protection such as secure channels between clients and the authentication server through Transport Layer Security (TLS).

IV. RECOGNITION-BASED CaRP:

For this type of CaRP, a password is a sequence of visual objects in the alphabet.

A. ClickText:

ClickText is a recognition-based CaRP patterns built on top of transcript Captcha. Its alphabet includes characters without any visually-confusing characters. For example, Letter “O” and digit “0” may cause confusion in CaRP images, and thus one character should be excluded from the alphabet. A ClickText password is a arrangement of characters in the script, e.g., $\rho =$“AB#9CD87”, which is related to a text password.

This is different from text Captcha task in which characters are usually ordered from left to right. in order for users to type them successively. a ClickText image with an alphabet of 33 characters. In entering a password, the user snaps on this image the characters in her password, in the same order, for example “A”, “B”, “#”, “9”,“C”, “D”, “8”, and then “7” for password $\rho =$“AB#9CD87”.

B. ClickAnimal

ClickAnimal is a recognition-based CaRP pattern built on top of Captcha Zoo, with an alphabet of alikeanimals such as dog, horse, Character identification is required in locating clickable points on a TextPoints image although the clickable points are known for each character. This is a task outside a bot’s capability.
B. TextPoints4CR
TextPoints can be improved to fit challenge-response authentication. This varies TextPoints for Challenge-Response or TextPoints4CR, pig, etc. Its password is a sequence of animal names such as \( \rho = \) “Turkey, Cat, Horse, Dog,...”

C. AnimalGrid
The number of similar animals is much less than the number of offered characters. ClickAnimal has a slighter alphabet, and thus a lesser password space, than ClickText. AnimalGrid’s password space can be increased by combining it with a grid-based graphical password, with the grid liable on the size of the selected animal.

VI. SECURITY ANALYSIS

A. Security of Underlying Captcha:
Computational intractability in identifying objects in CaRP images is fundamental to CaRP. surviving analyses on Captcha security were mostly case by case or used an exact process. A Captcha challenge typically contains 6 to 10 characters, whereas a CaRP image usually contains 30 or more characters.

B. Automatic Online Guessing Attacks:
In routine online predicting attacks, the trial and error process is performed automatically whereas dictionaries can be made manually.

C. Human Guessing Attacks
In human predicting attacks, users are used to enter passwords in the trial and error process. Humans are much slower than system in rising guessing attacks.

D. Relay Attack
Relay attacks may be performed in several ways. Captcha tasks can be relayed to a high-volume Website hacked or controlled by oppositions to have human surfers solve the challenges in order to continue surfing the Website, or relayed to sweatshops where users are hired to solve Captcha challenges for small payments.

E. Shoulder-Surfing Attacks
Shoulder-surfing attacks are a hazard when graphical passwords are entered in a public place such as bank ATM machines. CaRP is not hardy to shoulder-surfing attacks by itself.

F. Other:
CaRP is not secure to all possible attacks. CaRP is helpless if a client is compromised such that both the image and user-clicked points can be captured.
VII. EMPIRICAL EVALUATIONS

A. Implementations
ClickText and AnimalGrid were executed using ASP.NET. ClickText was implemented by calling a configurable text Captcha engine commercially used by Microsoft. This Captcha device accepts only capital letters.

B. Usability Study
1) Experimental Settings
We shown an in-lab usability study to compare Click-Text, AnimalGrid, PassPoints, text password (Text), and text password mutual with text Captcha (P + C). P + C was used to simulate a CbPA-protocol when a Captcha task was used in login.

2) Experimental Results
Usability. Among all the verified login attempts, 24.4% failed. Tests after a larger interval managed to have more failed attempts. Some participants contributed notably more failed attempts than others. At the end of tests, 40 (100%) participants retained their PassPoints passwords, 39 (97.5%) remembered their passwords of both ClickText and AnimalGrid, and 34 (85%) remembered their Text passwords.

VIII. BALANCE OF SECURITY AND USABILITY

Some designs of CaRP offer suitable usability across common device types, e.g. our usability studies used 400 × 400 images, which fit present of smart phones and computers.

A. Alphabet Size
Expanding alphabet size produces a larger password space, and thus is more protected, but also leads to more complex CaRP images.

A. Advanced Mechanisms
The CbPA-protocols described in Section II-C need a user to solve a Captcha challenge in addition to entering a password under certain conditions. The scheme described in applies a Captcha challenge when the number of failed login attempts has reached a threshold for an account.

IX. CONCLUSION

We have suggested CaRP, a new security primitive depend on unsolved hard AI problems. A password of CaRP can be found only probabilistically by automatic online guessing attacks including brute-force attacks, a chosen security property that other graphical password arrangements lack. Hotspots in CaRP images can no longer be exploited to support automatic real time predicting attacks. Overall, our work is one step forward in the paradigm of using hard AI problems for security. Of realistic security and usability and practical improvements, CaRP has good potential for modifications, which call for useful future work. More importantly, we think CaRP to motivate new discoveries of such AI based security primitives.

REFERENCES

d/ScienceBehindPassfaces.pdf


dnet.co.uk/news/networking/2002/03/26/hackers-
attack-ebay-accounts 2107350/


