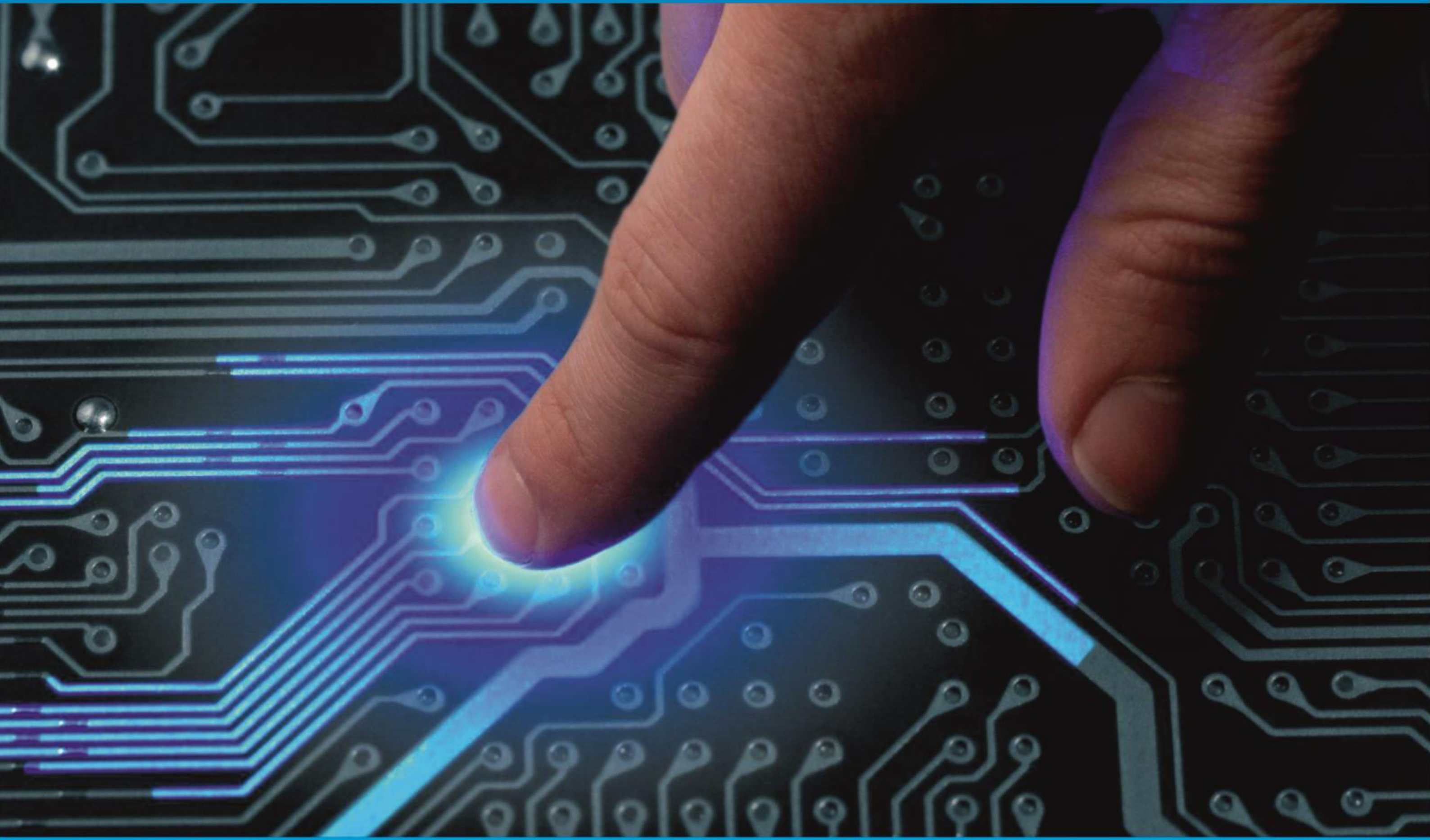
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE2021. 0903110|

Password Analysis Based on Secured Graphical Data Models of Image Choice and OTP

S. Satheesh Kumar[1], S.Ashika[2], B.Elavarasi[3], L.Johnsha[4]

AP, Department of IT, Vivekanandha College of Technology for Women Namakkal, India[1]

B. Tech, Department of IT, Vivekanandha College of Technology for Women, Namakkal, India[2,3,4]

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 underexplored. In this paper, we present a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Puzzle technology, which we call Puzzle as graphical passwords (CaPRP). CaPRP is both a Puzzle and a graphical password scheme. CaPRP 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 CaPRP password can be found only probabilistically by automatic online.

guessing attacks even if the password is in the search set. CaPRP 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.

CaPRP is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security.

I. OBJECTIVE

To design and development CaPGP to address a number of security problems altogether, such as online guessing attacks, relay attacks.It offers reasonable security and usability and appears to fit well with some practical applications for improving online security.

II. LITERATURE SURVEY

1.How to Attack Two-Factor Authentication Internet Banking, Manal Adham1, Amir Azodi1;3, Yvo Desmedt2;1, and Ioannis Karaolis1,March 2017

The original user-unfriendly approach of Barclays shows that if criminals would auto- mate their attacks, certain banks are ready to roll out their modifications and annul most of the attacks, the hardware/software used by most banks though, as HSBC and Bank of Cyprus, may not allow them to switch quickly. We observe that full transaction verification may not fully address all security concerns. The information displayed on the PC including; account numbers, name, balance and transaction details, do not remain private! Indeed, a browser rootkit can leak all this information to an attacker who could use it to physically target rich users, use identity theft techniques.

2.Two Factor Authentication Using Mobile Phones, FadiAloul, Syed Zahidi Department of Computer Science & Engineering American University of Sharjah, UAE {faloul, b00017408}@aus.edu March 2019

The implementation of two-factor authentication methods using mobile phones. It provides the reader with an overview of the various parts of the system and the capabilities of the system. The proposed system has two option of running, either using a free and fast connection-less method or a slightly more expensive smsbased method. Both methods have been successfully implemented and tested, and shown to be robust and secure. The system has several factors that makes it difficult to hack.

3.Users are not the enemy Anne Adams & Martina Angela Sasse Department of Computer Science University College London, January 2018

The key element in password security is the crackability of a password combination. Davies &Ganesan argue that an adversary's ability to crack passwords is larger than usually believed. System-generated passwords are essentially the optimal security approach; however, user-generated passwords are potentially more memorable and thus less likely to be disclosed (e.g. because users have write them down). The US Federal Information Processing Standards suggest several criteria for assuring different levels of password security. Password composition, for example, relates the size of a character set from which a password has been chosen to its level of security.

4.GraphicalPasswords:Learning from the First Twelve Years Robert Biddle, Sonia Chiasson, P.C. van Oorschot School of Computer Science Carleton University, Ottawa, Canada robert_biddle@carleton.ca, chiasson@scs.carleton.ca, paulv@scs.carleton.ca March 2017

multitude of graphical password schemes have been proposed, motivated by the promise of
improved password memorability and thus usability, while at the same time improving strength against guessing attacks. Like text passwords, graphical passwords are knowledge- based authentication mechanisms where users enter a shared secret as evidence of their identity. However, where text passwords involve alphanumeric and/or special keyboard char- acters, the idea behind graphical passwords is to leverage man memory for visual information.

5.The Quest to Replace Passwords:

A Framework for Comparative Evaluation of Web Authentication Schemes bJosephBonneau University of Cambridge Cambridge, UK jcb82@cl.cam.ac.uk Cormac Herley Microsoft Research Redmond, WA, USA cormac@microsoft.com Paul C. van Oorschot Carleton University Ottawa, ON, Canada paulv@scs.carleton.ca August 2016

The concise overview offered by Table I allows us to see high level patterns that might otherwise be missed. We could at this stage draw a variety of conclusions and note, for example, that graphical and cognitive schemes offer only minor improvements over passwords and thus have little hope of displacing them. Or we could note that most of the schemes with substantial improvements in both usability and security can be seen as incarnations of Single-Sign- On (including in this broad definition not only federated schemes but also “local SSO” systems [26] such as password managers or Pico). Having said that, we expect the longterm scientific value of our contribution will lie not as much in the raw data distilled herein, as in the methodology by which it was assembled.

III. EXISTING SYSTEM

Security primitives are based on hard mathematical problems. Using hard AI problems for security is emerging as an exciting new paradigm, but has been underexplored.A FUNDAMENTAL task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable.

DISADVANTAGES OF EXISTING SYSTEM:

- This paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications.
- Using hard AI (Artificial Intelligence) problems for security, initially proposed is an exciting new paradigm. Under this paradigm, the most notable primitive invented is Puzzle, which distinguishes human users from computers by presenting a challenge.

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 Puzzle technology,
which we call Puzzle as graphical passwords (CaPRP). CaPRP is both a Puzzle and a graphical password scheme. CaPRP 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 CaPRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. CaPRP 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. CaPRP 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 CaPRPs built on both text Puzzle and image-recognition Puzzle. One of them is a text CaPRP wherein a password is a sequence of characters like a text password, but entered by clicking the right character sequence on CaPRP images. CaPRP 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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903110|

ADVANTAGES 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. Defense against online dictionary attacks is a more subtle problem than it might appear.
- Puzzle Login(top of Puzzle technology Using mathematical problems).
- Image Puzzle Solving Using AES Algorithm.

IV. LIST OF MODULES

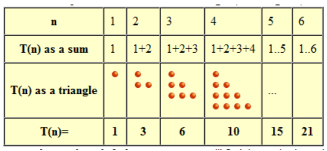
1.Puzzle Login
2.RandomCaptcha Selection
3.Image Puzzle Solving
4.OTP Generation
5.Online Bank

4.1 Module Descriptions:

1.Puzzle Login

The security and usability problems in text-based Login And password schemes have resulted in the development of Puzzle password schemes as a possible alternative.

We can visualize the sum 1+2+3+...+n as a triangle of character . Numbers which have such a pattern of character are called Triangle (or triangular) numbers, written T(n), the sum of the integers from 1 to n time Using Factorial base Login Puzzle Solving.



n	1	2	3	4	5	6
T(n) as a sum	1	1+2	1+2+3	1+2+3+4	1..5	1..6
T(n) as a triangle	●	● ● ●	● ● ● ● ● ●	● ● ● ● ● ● ● ● ● ●	...	
T(n)=	1	3	6	10	15	21

2. RandomCaptcha Selection

A CAPTCHA is a test that is used to separate humans and machines. CAPTCHA stands for "Completely Automated Turing test to tell Computers and Humans Apart." It is normally an image test or a simple mathematics problem which a human can read or solve, but a computer cannot. It is made to stop computer hackers from using a program to automatically set up hundreds of accounts, such as email accounts. It is named after mathematician.

Each individual is chosen randomly and entirely by chance, such that each individual has the same probability of being chosen at any stage during the sampling process, and each subset of n individuals has the same probability of being chosen for the sample as any other subset of n individuals This process and technique is known as simple random sampling, and should not be confused with systematic random sampling. A simple random sample is an unbiased surveying technique.

3.Image Puzzle Solving

we study how to prevent DoS/DDoSattackers from inflating their puzzle-solving capabilities. To this end, we introduce a new client puzzle referred to as software puzzle. Unlike the existing client puzzle schemes, which publish their puzzle algorithms in advance, a puzzle algorithm in the present software puzzle scheme is randomly generated only after a client request is received at the server side and the algorithmis generated such that: 1) an attacker is unable to prepare an implementation to solve the puzzle in advance and

2) the attacker needs considerable effort in translating a central processing unit puzzle software to its functionally equivalent GPU version such that the translation cannot be done in real time. Moreover, we show how to implement software puzzle in the generic server-browser model.

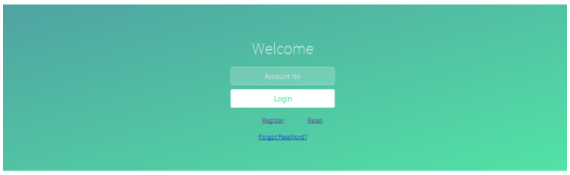
4.OTP Generation

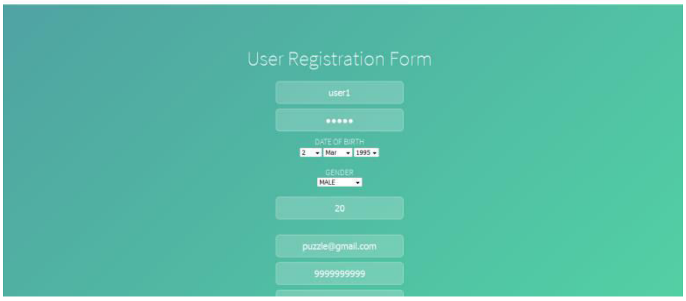
A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to something a person has (such as a small keyring fob device with the OTP calculator built into it, or a smartcard or specific cellphone) as well as something a person knows (such as a PIN).

5.Online Bank

Online banking also known as internet banking, e-banking, or virtual banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking that was the traditional way customers access banking services.

Screen Shots:





User Registration Form

user1

●●●●●

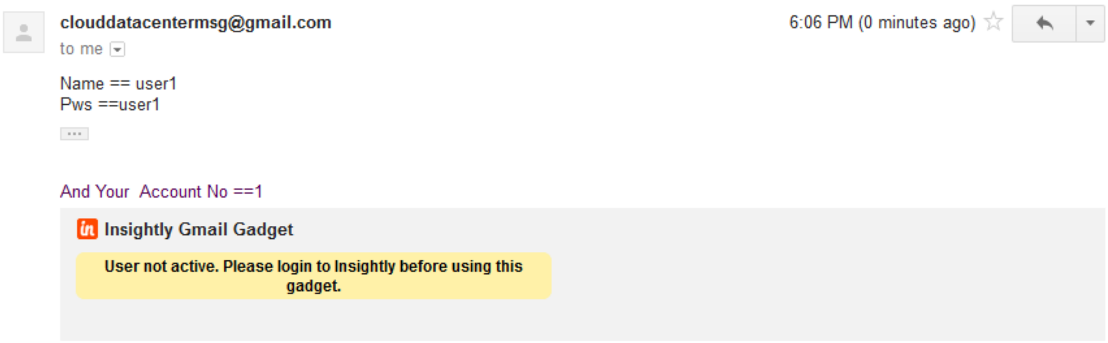
DATE OF BIRTH
2 Mar 1995

GENDER
MALE

20

puzzle@gmail.com

9999999999



clouddatacentermsg@gmail.com
to me

6:06 PM (0 minutes ago)

Name == user1
Pws ==user1

And Your Account No ==1

Insightly Gmail Gadget

User not active. Please login to Insightly before using this gadget.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903110|

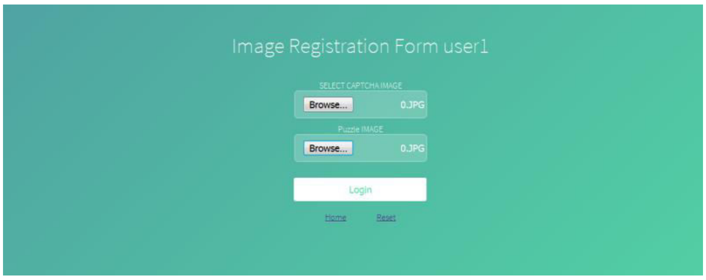
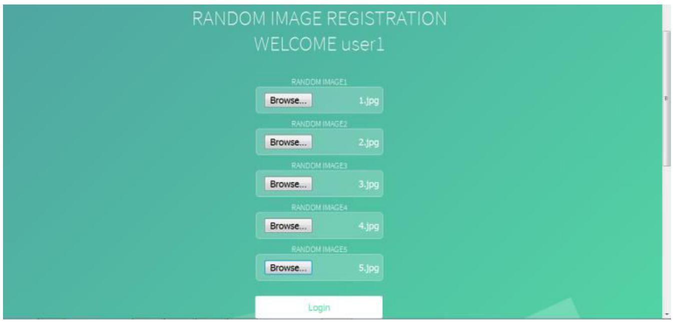


Image Registration Form user1

SELECT CAPTCHA IMAGE: 0.JPG

Puzzle IMAGE: 0.JPG



RANDOM IMAGE REGISTRATION
WELCOME user1

RANDOM IMAGE1: 1.jpg

RANDOM IMAGE2: 2.jpg

RANDOM IMAGE3: 3.jpg

RANDOM IMAGE4: 4.jpg

RANDOM IMAGE5: 5.jpg

V. CONCLUTION AND FUTURE WORK

5.1 CONCLUSION

the software puzzle may be built upon a data puzzle,it can be integrated with any existing server-side data puzzle scheme, and easily deployed as the present client puzzle schemes do. CAPTHCHA is widely research field act as internet rectifier to secure web applications by discern human from bots. CAPTCHA presented which will improve resistance of math calculus CAPTCHA. By use, Boolean operations and expressions instead of trigonometric and differential function which will help in reduce the complexity of CAPTCHA and help to achieve better usability and security as compared to math calculus CAPTCHA. Boolean CAPTCHAcan be easily use by educated user. No need of technical skill, by using intellectual
mind to solve this CAPTCHA and help to reduce time complexity.

5.2 Future work:

Captcha. In the authors propose using machine learning classi-fiers to attacks captchas. In the same authors study how efficientstatistical classifier are at recognizing captcha letters. In theauthors study how good humans are at solving well-known captchasusingMechanica Detecting and removing lines is a well studied field in computer vision since the '70s. Two well-known andefficient algorithms that can be used against captchas with lines are the Canny detection and the Hough Transform Removing noise using a Markov Random Field (Gibbs) was introduced in Many image descriptors have been proposed over the last decades: one of the first and most used descriptors is the the Harris Cornerdetector introduced . However, recently it has beenreplaced by more complex descriptors that are insensitive to scalend rotation (to a certain extent).

REFERENCES

[1] A. Adams and M. Sasse, "Users are not the enemy," Commun. ACM, vol. 42, pp. 40–46, 1999.
[2] M. Adham, A. Azodi, Y. Desmedt, and I. Karaolis, "How to attack twofactor authentication internet banking," in Proc. 17th Int. Conf. Financial Cryptography, 2013, pp. 322–328.
[3] ARTigo, http://www.artigo.org/.
[4] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," Proc. Comput. Syst. Appl., 2009, pp. 641–644.
[5] R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys vol. 44, no. 4, p. 19, 2012.
[6] G. E. Blonder, "Graphical passwords," U.S. Patent 5 559 961, 1996.
[7] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in Proc. IEEE Symp. Security Privacy, 2012, pp. 553–567.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING