International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Implementation of VSK and Arithmetic OTP Verification for Resisting Shoulder Surfing Attack

Shreyal Deshmukh[1], Priyanka More[2]

[1]M.E Student, G.S.Moze, College of Engineering, Pune, Savitribai Phule Pune University

[2]Professor, Computer Department, G.S.Moze, College of Engineering, Pune, Savitribai Phule Pune University

Abstract: ***Currently Cyber security is an important issue to tackle. A wide security primitive depend on hard challenges that can be computationally solved only by mathematical algorithms operations. Different user authentication methods are used for this purpose. There are many drawbacks in alphanumeric passwords that they can be guessed very easily or can be hacked. Currently researchers have proposed different graphical techniques such as CAPTCHA, PCCP, CaRP, PassMatrix, VRK, OTP & LTP etc. 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 Captcha technology, which we call Captcha as graphical passwords (CaRP). CaRP is both a graphical password and a Captcha 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. This section makes a deep survey over the many existing systems and thereby makes a comprehensive evaluation of the existing techniques making us ready to propose a new technique system which eliminate the drawbacks of the previous systems. The paper describes and studies different application oriented graphical systems proposed earlier and tries to find the loopholes to avoid the attacks.***

Keywords: Password Attacks, CaRP, OTP, LTP, Captcha, Security, Graphical Password

1. Introduction

As we know that text password is very traditional method in the security system. Text passwords have been used massively in authentication method for decades. The main objective of the security is to create highly non forgeable primitives and cryptographic based on hard mathematical arithmetic formulations that are computationally intractable. For eg, the integer factorization system problem is basic to the RSA use of online transactions and online banking i.e. in ERP and E- Commerce have rapidly increased and Using difficult AI (Artificial Intelligence) challenges for security using Graphical Passwords public-key cryptographic system. In the previous decade, the, CAPTCHA system, initially design in [7], is an exciting new paradigm. Under innovative style, the widely used technique for security system invented is Captcha, which differentiate human users from computers by showing a challenge, i.e., a puzzle and many more systems related. Many ideas fail to get immunity towards shoulder surfing attacks and there for makes the system expose to attacks and thus making the password styles insecure and easy to hack.

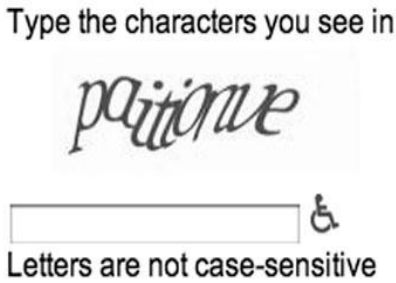


Figure: Text based Captch

Starting form 1999 [3], different graphical password schemes include as an option or alternatives to simple and easy text-based password authentication. This section paper provides analytical overview and comprehensive system of published research work in this domain, viewing the both the features such as security aspects, usability and along with that system opinion. This survey first documents the existing or already prevailing approaches, innovative and enlightening new features of the individual styles and finding the key features of security advantages or usability ease. This paper takes into account the usability parameters for knowledge-based authentication and authorization as being applied to pictorial secure passwords and detect the security issues getting addressed that these techniques must identify and analyze, discuss technical problems concerned with performance evaluation, and search the research areas for further improvement and study. With text based passwords or credentials, users try out for unsecure coping technique, like making use of exact passwords for different transactional accounts to avoid forgetting memorizing different passwords and avoiding the passwords for different his/her accounts, change in security level cannot be alone addressed by the basic technical security of the system. Major problems that actually impact significantly in real life are about usability of that system. GUI (Graphical User Interface) design strategies and approaches may intentionally or unintentionally sway users' behavior or tendency towards less secure transactional behaviors. Thus these most and powerful secure applications system must constraint high GUI related constraints based on necessary research work including the shortcomings and capabilities of the targeted users. In pictorial passwords, human nature for memorizing objects or visual passwords will provide appropriate and the optimal selection use of high level secure and passwords that have very low predictability, refraining users from unsecure practices.

2. Literature Survey

A fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. The author notice how an attacker might predict or infer the hot-spots that are examine for using in the dictionary attack (offline). While instead of using image processing system technique to guess hot-spots, this system rather uses human analyze, which totally depends on the people to perform various action that computers (at least at the present moment) find difficult to perform. Here author process this dataset to determine a few sets of points that are more usually and commonly considered first, to introduce an attack (human-seeded). A human-seeded attack in normal terms can be summarized as an attack generate with the help of data which is collected from the people. Author produce three different predictive pictorial dictionaries (i.e, depending upon the recently available data that relates to the user's login system process, gathered from various sources than the target database, where the target database is nothing but the set of user system passwords which are under attack): few based on various paradigms of seeded (human-seeded) attacks, and the different based on the rule of click-order patterns or styles. After evaluation of both study and the database of both the data sets, application system of a 10-fold cross-validation analysis with the past field study user password database to test and train few style of human attack, providing a scenario about how good the attacker will be familiar with such type techniques.

A. The design and analysis of graphical passwords

In this proposed system, to achieve better security than text based passwords we propose and evaluate new graphical password schemes that exploit features of graphical input displays. To decouple the position of inputs from the temporal order in which those inputs occur, Graphical input devices enable the user and we show that this decoupling can be used to generate password schemes with substantially larger password spaces. We devise a novel way to capture a subset of the \memorable" passwords in order to evaluate the security of one of our schemes that, we believe, is itself a contribution. In this work, we are primarily motivated by devices such as personal digital assistants (PDAs) that offer graphical input capabilities via a stylus, and we describe our prototype implementation of one of our password schemes on such a PDA, namely the Palm Pilot TM.

B. Graphical Passwords: Learning from the first twelve years

In this paper, the existing approaches catalogues first, novel features of selected schemes are highlighting and key usability or security advantages are identifying. For knowledge-based authentication we then review usability requirements as they apply to graphical passwords, identify security threats that such systems must address and review known attacks, related to empirical evaluation there discuss methodological issues, and identify areas for further research and methodology is improved.

C. Captcha as Graphical Password-A new security Approach Based on Hard AI Problems

Bin B.Zhu et al proposed CaRP scheme [1]. In CaRP i.e. CAPTCHA and graphical password both are used after combining and as a single entity for authentication. The CaRP schemes are actually click-based graphical passwords with the CAPTCHA technique used in a way that a new image is generated for every login attempt even for the existing user just as CAPTCHAs change every time.

D. A New Architecture for the Generation of Picture Based CAPTCHA

Automated network attack such as denial-of-service (DoS) leads to significant wastage of resources, which is a common threat to network security. To prevent these automated network attacks CAPTCHA based security mechanism is to be adopted so that it will differentiate humans from machines. Optical Character Recognition (OCR) based CAPTCHAs are more vulnerable to automated attacks due to the existence of correlation algorithms and di rect distortion estimation techniques. The illegibility of the text CAPTCHA makes the user difficult to read it and thus they feel uncomfortable .In order to overcome these difficulties a new type of CAPTCHA, that is, picture based CAPTCHAs came into existence, which are more efficient and secure than the existing text based CAPTCHAs. We propose a new architecture for the generation of picture based CAPTCHA, which is resistant to segmentation through edge detection and thresholding, shape matching and random guessing. Our security analysis shows that the proposed architecture is showing better results in comparison with other picture based CAPTCHAs.

E. One Time Password Security Measure

An OTP [6] is a password as the name suggests that is valid scheme for authentication to next process of only one login transaction or session with the system. OTPs remove a number of shortcomings or limitations that are same with alphanumeric old and commonly used "static" passwords. Limitation or shortcoming that is overcome or noticed by OTPs is in contrast to generally used alphanumeric static passwords, they are not prone or vulnerable to replay attacks. That means even a potential intruder who can analyze to record an OTP somehow if possible, that was already previously used to log into a service or the system or to conduct a transaction will not be able to forge it since, it will be no longer valid data for transaction. On the other section, OTPs are also difficult for us to remember for long time. Therefore they require advance technology to work. How to generate OTP code and distribute to the individual user? OTP distribution and generation algorithms generally make use of pseudo randomness. This is necessary because if we don't do so, it would be very easy and simple to guess future generated OTPs by analyzing and observing the previous ones. Random and concrete OTP algorithms vary smartly in their workings.

There are also different ways or mediums to make the user aware of the next OTP to use. Some One Time Password

generation systems [7] use special type electronic security tokens or equipment which user take and then these systems generate OTPs and show it using a small LCD display device. Other OTP generation systems consist of various kind of software that runs on the client's or user's cell phone. But the lasting systems and the most secure system to generate OTPs on the server side and after that send these OTPs to the user using some out-of-band communication channels or mediums such as emails or SMS. In some banking activation systems and transaction system, OTPs are printed on high secure barcoded paper which user has to carry.

Certain type cryptography algorithms in the communication system, by their mathematical properties cannot be fake by brute-force and e.g., of this secure way is the one time password (OTP) algorithm [7], where individual plain text bit has an equivalent and corresponding key bit. One-time passwords or OTPs depend on the capability to produce the actual new and unique random sequence of key bits. Brute force attack would gradually show the original decoding, and also all the other possible combinations of bits and would have no medium of differentiating one from another. A very little i.e. 100-byte, one-time-password (OTP) encoded string considered for a brute force attack would truly reveal every 100-byte string possible, including the original OTP as an answer, but with very low probability. Now the analysis of one-time password (OTP) algorithm for safe and secure transactions over the network available today based on email authentication or mobile authentication is completed and also the analysis of the possible attacks over the one-time password (OTP) algorithms have studied.

In the existing one time password [7] OTP algorithm, java mobile midlet is client application and now we further assume that the client application runs in client's cell phones/ mobile phones which will be able to receive one time passwords (OTP) during login requests. A MIDlet is a java based application that prepares use of the Mobile Information Device Profile (MIDP) of the technology known by Connected Limited Device Configuration (CLDC) for the Java Mobile Environment (JME). Typical applications using MIDLets include games running on cell phone devices or any other handheld devices and mobile phones which have little graphical displays, simple alphanumeric or numeric interfaces and limited but allowable network access over hypertext mark-up language (HTTP). The whole design system resembles the two prime protocols used by Java system. In the first stage, the user has to download the clients (Java MIDlet) to his cell phone or any other handheld devices. After that the client application can executes a request to register with both the service provider and the server utilizing server system for generating one time password and user authentication. Previous successful execution of the user activation request, the user can run authentication request in future for an unlimited number of times.

3. Proposed System

- The propose system proposes 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.
- Captcha as graphical passwords (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.
- Captcha as graphical passwords, CaRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set.
- CaRP also provide 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.

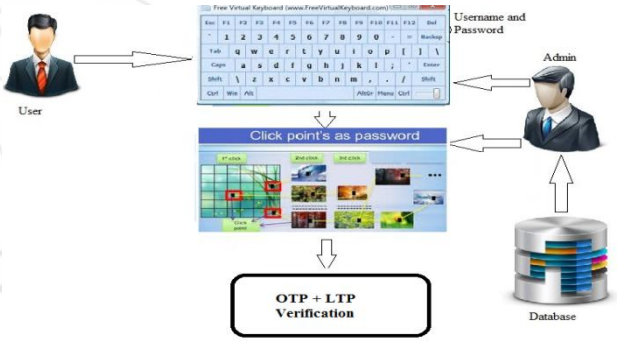


Figure 1: Proposed system architecture

A. Virtual Random Keyboard:
Virtual random keyboard is a technique used to avoid the shoulder surfing attack by randomly shuffling the characters from the QWERTY keyboard so that the attacker cannot guess the characters getting pressed while typing the password.

B. Pass Matrix Module:
Multiple images of different levels of difficulty based on log in history of the user and machine is used for providing Carp images. The proposed system focuses on major attacks such as shoulder surfing and password guessing by introducing two major novel techniques:

C. OTP with LTP Authentication:
One time password is combined long time password. These Passwords are sent to user's mobile via message and on emailed via email.OTP is different every time, LTP remains constant.

4. Mathematical Model

In the mathematical operation we will see the operations of the modules of the system with the set theory applied to the project.

Set theory applied to the project:

Captcha a graphical password scheme:
Set (P) = {p0, p1, p2, p3, p4, p5, p6, p7, p8}
P0=get user registration details
P1=alphanumeric password for first level authentication
P2=captcha graphical image authentication
P3=keyboard orientation authentication
P4= attacker module

User module:
Set (R) = {p0,p1,f0,f1}
f0= Get user Name
f1=get user password.

Alphanumeric Password:
Set (A) = {p1,d0,d1,d2}
d0= Enter alphanumeric password
d1= confirm alphanumeric password
d2=Submit registration details

CAPTCHA Graphical image authentication:-
Set (C) = {p1,p2,e0,e1,e2}
e0= Select Images as graphical passwords
e1= click of random points on images
e2=Save the Cued Click points in database.

Keyboard Orientation Authentication:-
Set (K) = {p2,g0,g1,g2}
g0=click keywords on onscreen keyboard
g1=change keyboard orientation every time
g2=save the keywords entered.
Set (C) = { p1,p2,e0,e1,e2}
Set (K) = { p2,g0,g1,g2 }
Set (A) = {p1,d0,d1,d2}
Set (R) = {p0,p1f0,f1}

Vein Diagrams

(P U R)= {p0, p1, p2, p3, p4, f0, f1}

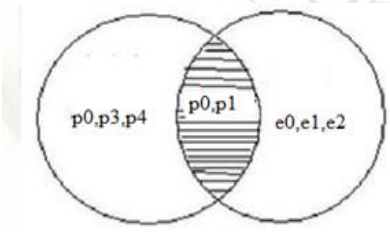


Figure 3: (P intersection C) = {p1,p2}

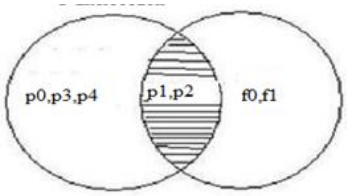
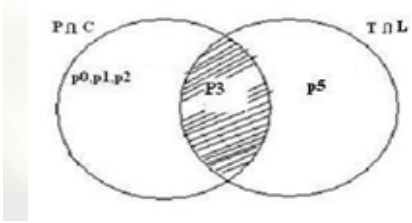


Figure 4: (P intersection R)= {p0, p1}



5. Results

Results of proposed system are as given below:

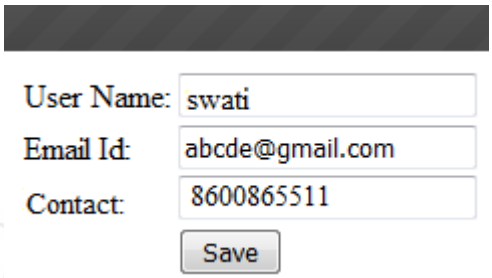


Figure 5: User's Login

Figure 6: Select Image Pixel Values

Figure 7: Enter OTP for Verification

6. Conclusion

We have proposed CaRP, a new security primitive relying on unsolved hard AI problems. Now, analyzing the existing pictorial or graphical login techniques such as PCCP or CaRP or CCP OTPs (including cellphone client based one time password and Server side generated OTPs), the need for some more additional and efficient authentication systems gives rise to the improvement of the designed system which has two advance features for user authentication other than PCCP or CARP. Proposed system comprise of the advanced LTP OTP incorporation for authenticating user along with OTP and Long term password (LTP) backend mathematical calculation and Virtual random keyboard for removing shoulder surfing attack. Existing systems thereby fail to provide 100% efficiency in providing secure and safe graphical passwords system and hence are vulnerable to

attacks such as shoulder surfing attacks and dictionary attacks.

References

[1] Bin B.Zhu, Jeff Yan, Gunabo Bao, Maowei Yang and Ning Xu, "Captcha as Graphical Password-A new Security Approach Based on Hard AI Problems", IEEE,June 2014.
[2] Phen-Lan Lin, Li-Tung Weng and Po-Whei Huang, "Graphical passwords using images with random tracks of geometric shapes," 2008 Congress on Images and Signal Processing, 2008.
[3] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme", in 21st International Conference on Advanced Information Networking and Applications Workshops, vol.2. Canada, 1999, 2007, pp. 467-472.
[4] 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.
[5] P. C. van Oorschot and J. Thorpe, "Exploiting predictability in clickbased graphical passwords," J. Comput. Security, vol. 19, no. 4, pp. 669–702, 2011.
[6] E.Kalaikavitha, Juliana gnanaselvi, "Secure Login Using Encrypted One Time Password (Otp) and Mobile Based Login Methodology," Research Inventy: International Journal Of Engineering And Science Vol.2, Issue 10 (April 2013), Pp 14-17.
[7] S. Benson Edwin Raj, Deepa Devassy and Jiji Jagannivas A New Architecture for the Generation of Picture Based CAPTCHA, IEEE, pp. 67-71, 2011.
[8] Viju Prakash, Alwin Infant, S. Jeya Shobana, "Eliminating Vulnerable Attacks Using One-Time Password and PassText-Analytical Study of Blended Schema", Universal Journal of Computer Science and Engineering Technology 1 (2), 133-140, Nov. 2010. © 2010 UniCSE, ISSN: 2219-2158.
[9] 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.
[10] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. ESORICS, 2007, pp. 359–374.
[11] David Kim, Paul Dunphy, and Pam Briggs, "A Shoulder Surfing Resistant Visual Authentication Scheme," (Volume:PP , Issue: 99), April 10-15, 2010.