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

A Comprehensive Survey on Various Graphical Password Schemas against Shoulder Surfing Attack

Priyanka Kokate[1], H.B. Jadhav[2]

[1] Vishwabharati Acadamy's College of Engineering, Ahmednagar, Savitribai Phule Pune University

[2]Assistant Professor, Vishwabharati Acadamy's College of Engineering, Ahmednagar, Savitribai Phule Pune University

Abstract: ***A massive security primitives depend on hard challenges that can be computationally solved only by mathematical algorithms operations. There are many drawback in alphanumeric passwords that they can be guessed very easily or can be hacked. So recently many researchers have proposed different graphical techniques such as CaRP, CAPTCHA, PCCP etc. This section makes a deep survey over the many existing systems and thereby make 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 describe 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

A basic goal 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 E- Commerce and ERP 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 idea fail to get immunity towards shoulder surfing attacks and therefor makes the system expose to attacks and thus making the password styles insecure and easy to hack.

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 survey the 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 tendency for memorizing objects or visual passwords will facilitate 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

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.

3. Graphical Password

Graphical password technique is a great innovation and an exact alternative to alphanumeric passwords technique in which users are given a challenge to click on pictures or images to authenticate themselves, instead of typing text or alphanumeric words which are easily guessed [3]. These type of graphical passwords are more memorable, as memorizing scenes or images are easier than memorizing difficult alphanumeric passwords, compared to the text or alphanumeric passwords. Previous psychological researches have experimentally and evidently proved that human minds are friendlier with memorizing video or images rather than combination of, numbers and alphabets in a random way [4]. For textual passwords, we have to first notice the text term, make out a systematic representation out of it and then memorize it as a passwords, which is comparatively difficult. Therefore, Using pictures or images instead of numbers or alphabets will help the user to increase the security constrain as the alpha-numeric corpus size is limited because of limited combinations and permutation. But in the case of graphical password system, the corpus size is large or infinity, if it is in the case of multiple numbers of images or if it is in the case of multiple points in a single pictures [5]. But another way round, we can select only 10 numbers and 26 alphabets textual case of alphanumeric password system.

4. Graphical Password Methods

In this part, we analysis of previously and the existing researched graphical password system methods are discussed. Pictorial or graphical password techniques are mostly proposed to overcome the easiest limitations of the conventional number or text based password techniques or styles, because images are easier to remember rather than textual passwords. It is known as Picture superiority effect [2]. A literature and previous study of other proposed papers regarding Graphical password techniques imply that the techniques can be classified or grouped into groups as follows (Fig.1)-

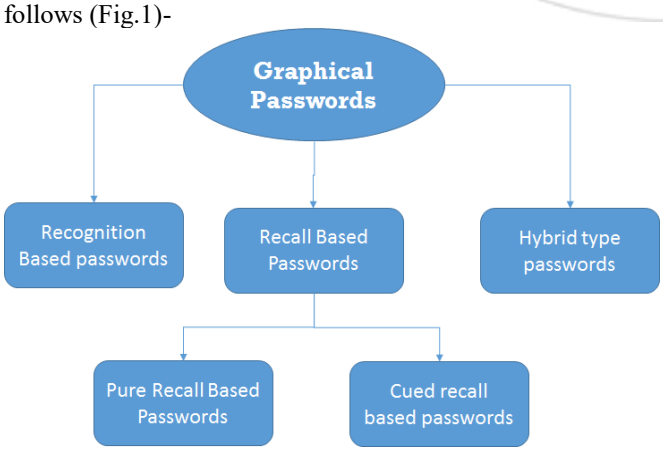

Figure 1: Types of graphical passwords

A. Recognition style Passwords

In this section, during registering time to the system, users have to select images, pictures, icons or symbols from a collection of different images. At the time of authentication, the users require to recognize their pictures, symbols or icons which are selected at registration time among a set of images. Researches were done to detect the memorability of these passwords and it express that the users can memorize his passwords even after 45 days [4]

B. Pure Recall-Based Technique

With this type of category, users trying to login to the system has to regenerate or reproduce their login passwords without being provided any type of reminder or hint. This category is easy and simple way, but it forces users to remember the passwords that users can hardly remember. But still it is comparatively more secure rather than the past recognition based system.

C. Cued Recall-Based Technique

With this section, users have an option with the help of hints or reminders for login passwords. Such type reminders aid the users in regenerating their login passwords or help users to quickly memorize the passwords by the hints. This paradigm is similar to the recall system based techniques but it is recall along with cueing.

D. Hybrid Schemes

With this part, the user login authentication will be normally the combination of difficult combination of two or more styles. Such combinational are mostly used to overcome the silly drawbacks of a single output schemes, such as spyware shoulder surfing and so on.

5. One Time Password Security Measure

An OTP (one-time password) [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. The vital 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 consists 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. Finally, in few 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. The example 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. A brute force attack would gradually reveal 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 cellphones/ mobile phones which will be able to receive one time passwords (OTP) during login requests. A MIDlet is a java based application that prepare 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 cellphone 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 markup 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 cellphone 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 no. of times.

6. Pervasive Cued Click Points

Existing graphical systems have clearly showed that picture hotspots are more prone to be predicted, which leads to less secure graphical passwords or image and thereby improve the security breach using dictionary attacks [10]. The survey determined if password selecting ability could be affected by making users to select any random click-points but still managing the usability. The designed system aim is to compel compliance by making the insecure task (i.e, choosing poor or weak strength passwords) more and more time-consuming and tedious. Thus, path of resistance for being secure and safe became less. So using the predefined CCP system as a base system, this system additionally shows a persuasive feature to make the users to select many secure passwords, and to make it very difficult to select passwords which will remove all five click points to be hotspots, especially when the people trying to login in created the password and the picture was shaded for creating the viewport. The viewport, in original, is placed randomly instead of individual sequence, so as to avoid the generally used hotspots, as this kind of information can be largely utilized by the dictionary attackers which can also consequently create new hotspots.

[9] The original viewports size was intentionally kept so as to offer a various variety of click points but also cover only the acceptably little amount or a fraction of all the possible points to be clicked. It was necessary for users to click within the highlighted portion and not out of the highlighted area part. If the users not able to manage to click within the highlighted portion, users were supposed to click the shuffle button portion so as to reposition the highlighted portion or the viewport. Facility to shuffle the viewport thereby increasingly made process of password creation lengthy. Password making phase only had the facility or using the shuffle and change viewport option but while user log-in and password confirmation, pictures that were displayed were without any shades or distortion or no highlighting of specific portions and the clicks were allowed anywhere.

7. Conclusion

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. The proposed system comprise of the advanced OTP LTP incorporation for authenticating user along with OTP and Long term password (LTP) backend mathematical calculation and Virtual random keyboard for removing shoulder surfing attack. The existing systems thereby fail to provide 100 percent efficiency in providing secure and safe graphical passwords system and hence is vulnerable to attacks such as shoulder surfing attacks and dictionary attacks.

References

[1] 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.

[2] K. Renaud and E. Smith. Jiminy: "Helping user to remember their passwords". Technical report, School of Computing, Univ. of South Africa, 2001.
[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, 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] 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.
[8] 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.
[9] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. ESORICS, 2007, pp. 359–374.