Survey paper on CAPTCHA AND VRP

Vijayalaxmi Daundkar, Prashant Kumbharkar
Siddhant College Of Engineering,
Sudumbre,Savitribai Phule Pune University.

ABSTRACT:- **A Lot of security primitives are based on hard challenges that are solvable only by mathematical formulations. Use of Difficult AI problems for security has become an evolution for a new paradigm of security, but still left underexplored. In this paper, we will noticeably present a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on the basis of Captcha technology, which we call Captcha as graphical passwords (CaRP). CaRP is a complex combination of Captcha and a graphical password style. 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. CaRP alone becomes inefficient to prevent all security, hence this paper makes a survey of the various security measures for secure password schemes and gives a clear picture of the efficiencies of the different techniques. There is no panacea, but highly secure password offers reasonable security and usability and appears suit well with practical applications for improving online security.**

Index Terms **: CaRP, OTP, Graphical Password, Captcha, Security, Password Attacks.**

1. Introduction

A basic aim of the security is to create cryptographic and highly non forgeable primitives based on hard mathematical formulations that are computationally intractable. For example, the integer factorization problem is basic to the RSA public-key cryptographic system. In the past decade, the use of online banking and online transactions i.e. in E-Commerce have rapidly increased and Using difficult (Artificial Intelligence) AI challenges for security using CAPTCHA, Graphical Passwords, initially proposed in [7], is an exciting new paradigm. Under this innovative style, the mostly used technique for security invented is Captcha, which distinguishes human users from computers by presenting a challenge, i.e., a puzzle. Many techniques fail to achieve immunity towards shoulder surfing attacks and therefor makes the system vulnerable to attacks and thus making the password styles insecure.

Beginning from around 1999 [3], various graphical password schemes evolved as alternatives or an option to simple and text-based password authentication. This paper provides a comprehensive and analytical overview of published research work in this domain, analyzing the both the features such as usability, security aspects, and along with that system evaluation. This survey first documents the existing or already prevailing approaches, enlightening new and innovative features of the particular styles and determining the key features of usability ease or security advantages. This survey the takes into account the usability parameters for knowledge-based authorization and authentication as being applied to pictorial secure passwords, detect the security issues getting addressed that these techniques must verify and analyze, discuss technical issues concerned with performance evaluation, and detect the research areas for further study and improvement. With textual passwords or credentials, users try out for unsafe coping strategies, like making use of same passwords for multiple transactional accounts to avoid forgetting the passwords and avoiding memorizing different passwords for different accounts, change in security level cannot be alone addressed by the underlying technical security of the system. Major issues that actually impact significantly in real life are about usability. GUI design approaches and strategies may intentionally or unintentionally sway users' tendency or behavior towards less secure transactional behaviors. Thus these powerful and most secure applications must constraint high GUI related constraints based on essential research work considering the capabilities and shortcomings of the targeted users. In pictorial passwords, human tendency for memorizing visual passwords or objects will facilitate the optimal selection and appropriate use of highly secure and passwords that have very less predictability, refraining users from unsafe practices.

2. Literature Survey

The author addresses how an attacker might infer or predict the hot-spots that are observed for using in the dictionary attack (offline). Instead of using image processing technique to predict hot-spots, this system rather uses "human computation", which depends on the people to perform various tasks that computers (at least at the current moment) find complicated to perform. Author here process this dataset to find out a few sets of points that are more commonly and usually considered first, to generate an attack (human-seeded). A human-seeded attack in general terms can be summarized as an attack produced with the help of data which is collected from the people. Author generates three various predictive pictorial dictionaries (i.e., depending upon the currently available data that relates to the user's login process, gathered from sources outside of the target password database itself, where a target password database is the set of user passwords under attack): two based on different styles of human-seeded attacks, and another based on click-order patterns. We evaluate these dictionaries, and also combined human-seeded and click-order pattern attacks, using our field study data set. We also perform a 10-fold cross-validation analysis with our field study database to train and test one style of human-seeded attack (based on a first-order Markov model), providing a sense of how well an attacker might do with these methods and an ideal human-computed data set for training. Author's contributions include an in-depth study of hot-spots in click-based (and cued-recall) graphical password schemes, and the impact of these hot-spots on security through two separate user studies. We explore predictive methods of generating attack dictionaries for click-based graphical passwords. Perhaps our most interesting contribution is proposing and exploring the use of human-computation to create graphical dictionaries; we conjecture that this method is generalizable to other types of graphical passwords (e.g., recognition-based) where users are given free choice.

3. Graphical Password

Graphical password is a great innovation and an absolute alternative to alphanumeric passwords in which users are given a challenge to click on images to authenticate themselves, instead of typing alphanumeric words which are easily guessed [3]. These Graphical passwords are more memorable, as memorizing images or scenes are easier than memorizing complex alphanumeric length passwords, compared to the alphanumeric passwords. Past psychological researches have experimentally and evidently proved that human brains are more friendly with memorizing images or video rather than combination of alphabets and numbers in a random fashion [4]. For textual passwords, we have to first analyze the text, make out a semantic representation out of it and then remember it as passwords, which is comparatively tedious. Therefore, Using images or pictures instead of alphabets or numbers will help the user to improve the security constrain as the alphanumeric corpus size is limited due to limited permutation and combinations. But in the case of graphical password, the corpus size is 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 image [5]. But the other way round, we can select only 26 alphabets and 10 numbers textual case of alphanumeric password.

4. Graphical Password Methods

In this section, we, the analysis of the existing and previously researched graphical password methods are discussed. Graphical or pictorial password techniques are widely proposed to overcome the simplest limitations of the conventional text or number based password styles or techniques, because pictures are convenient to remember than textual passwords. It is called as "Picture superiority effect" [2]. A literature and past survey of other proposed papers regarding graphical password techniques imply that the techniques can be grouped or classified into groups as follows (Fig.1):

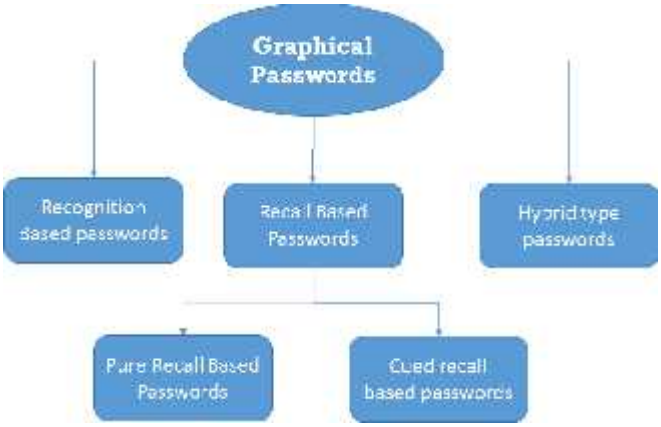

Figure 1: Types of graphical passwords.

A. Recognition style Passwords:

In this category, during registering to the system, users have to select images, icons or symbols from a collection of images. At the time of authentication,

the users need to recognize their images, symbols or icons which are selected at the time of registration among a set of images. Researches were done to find the memorability of these passwords and it shows that the users can remember their passwords even after 45 days [4].

B. Pure Recall-Based Technique:

With this category, users trying to login to the system has to reproduce their login passwords without being provided any type of hints or reminder. Even though this very category is easy and convenient way, but it forces users to memorize the passwords that users can hardly remember. But still it's comparatively more secure than the recognition based system.

C. Cued Recall-Based Technique:

With this category, users are facilitated with the help of reminders or hints for login passwords. Such Reminders aid the users in reproducing their login passwords or help users to quickly remember the passwords through the hints. This paradigm is quite similar to the recall based techniques but it is recall along with cueing.

D. Hybrid Schemes:

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

5. One Time Password Security Measure

A one-time password (OTP)[6] is a password as the name suggests that is valid for authentication of only one login session or transaction with the system. OTPs avoid a number of limitations or shortcomings that are related with alphanumeric traditional and commonly used (static) passwords. The major limitation or shortcoming that is noticed or overcome by OTPs is, in contrast to commonly used alphanumeric static passwords, they are not vulnerable or prone to replay attacks. That means even a potential intruder who can manage to record an OTP somehow if possible, that was already previously used to log into the system or a service or to conduct a transaction will not be able to forge it, since it will be no longer valid for transaction. On the other side, OTPs are also quite difficult for us to memorize for longer time. Therefore they require additional technology to work. How to generate OTP and distribute to the particular user? OTP generation and distribution algorithms generally make use of pseudo randomness or randomness. This is essential because if we don't do so, it would be very simple and easy to predict future generated OTPs by observing and analyzing the previous ones. Concrete and random OTP algorithms vary greatly in their workings.

There are also various mediums or ways to make the user aware of the next OTP to use. Some OTP generation systems[7] use special equipment or electronic security tokens which user carries and then these systems generate OTPs and show it using a small LCD display. Other OTP Generation systems consists of some kind of software that runs on the user's or client's mobile phone. But the most secure and lasting systems generate OTPs on the server-side and then send these OTPs to the user using some out-of-band communication channels such as SMS or emails. Finally, in some banking transaction and activation systems, OTPs are printed on secure barcoded paper which user has to carry.

Certain type cryptographic algorithms in the communication networks, by their mathematical properties cannot be forged by brute-force. The best example of this secure way is the one-time password algorithm (OTP)[7], where every plain text bit has a corresponding and equivalent key bit. One-time passwords or OTPs depend on the capability to generate the actual new and very unique random sequence of key bits. A brute force attack would gradually reveal the actual decoding, and also all the other possible combinations of bits, and would have no way of differentiating one from the another. A very small, i.e. 100-byte, one-time-password encoded string considered for a brute force attack would literally reveal every 100-byte string possible, including the actual OTP as an answer, but with least probability. Here the analysis of one-time password algorithm for a secure transactions over network available today based on mobile authentication or email authentication is completed and also the analysis of the possible attacks over the one-time password algorithms have studied.

In the existing (OTP)[7] one-time password algorithm, java Mobile midlet is a client application and we further assume that the client application runs in client's mobile phones/cellphones which will be able to receive one time passwords during login requests. A MIDlet is a java based application that makes use of the Mobile Information Device Profile (MIDP) of the technology called Connected Limited Device Configuration (CLDC) for the Java Mobile Environment (ME). Typical applications using

MIDLets include games running on mobile devices or other handheld devices and cell phones which have small graphical displays, simple numeric or alphanumeric keypad interfaces and limited but allowable network access over HTTP. The whole design resembles the two prime protocols used by Java system. Initially, the user has to download the clients (Java MIDlet) to his mobile phone or other handheld devices. Then the client application can executes a request to register with both the server and the service provider utilizing server system for generating OTP and user authentication. Post successful execution of user activation request, the user can run the authentication request in future for an unlimited number of times.

6. Pervasive Cued Click Points

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

[10]The actual viewports' size was intentionally kept so as to offer a different variety of click points but also cover only the acceptably small amount or a fraction of all the possible points to be clicked. Users were required to select a click-point within this highlighted viewport and could not click outside of this viewport. If they were unwilling or unable to select a click-point in this region, they could press the "shuffle" button to randomly reposition the viewport. While users were allowed to shuffle as often as they wanted, this significantly slowed the password creation process. The viewport and shuffle buttons only appeared during password creation. During password confirmation and login, the images were displayed normally, without shading or the viewport and users were allowed to click anywhere.

7. Conclusion

Thus after analyzing the existing graphical or pictorial login techniques such as CaRP, or CCP or PCCP r OTPs (including mobile client based OTPs and Server side generated OTPs), the need for some more advanced and efficient authentication systems gives rise to the implementation of the proposed system which has two additional features for user authentication other than CARP or PCCP. The proposed system comprise of the advanced LTP OTP incorporation for authenticating user along with OTP and LTP backend mathematical computation and Virtual Random Keyboard for avoiding shoulder surfing attack. The existing systems thereby fail to provide 100% efficiency in providing secure graphical passwords and hence is vulnerable to attacks such as shoulder surfing, 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.

[10] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: Persuasive cued click-points," in Proc. Brit. HCI Group Annu. Conf. People Comput., Culture, Creativity, Interaction, vol. 1. 2008, pp. 121–130.