INTELLIGENT PASSWORD AUTHENTICATION FOR AVOIDING SHOULDER SURFING AND BRUTE FORCE ATTACKS

Mrs. Arti Suryavanshi
Department of Computer Engineering, VACOE, Ahmednagar, India

Prof. Prashant Suryavanshi
Department of Computer Engineering, HSBPVTGOIPCOE KASHTI, Shrogonda, India

Prof. Mrs. Vidya Jagtap
Department of Computer Engineering, VACOE, Ahmednagar, India

ABSTRACT

Tremendous security measures are based on difficult challenges that can be solved only by mathematical computations and analysis. Latest paradigm for higher security is based on hard artificial Intelligence problems, yet unexplored. In this paper, A novel technique of authenticating users through virtual random keyboards and two level intelligent authentication is accrued out, which we can call as combination of Captcha as a graphical password (CaRP) and VRK. CaRP is a complex and innovative technique using graphical style password. CaRP solves the issues of a number of attacks, such as online guessing attacks, relay attacks, shoulder-surfing attacks etc. 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.

INTRODUCTION

Security measures aim in determining a highly cryptographic technique using various hard AI based mathematical formulations and computations. For an instance, factorization of integers is very basic problem which can be easily breached by attackers. Ecommerce, or online trading banking has boosted since last decade and hence the use of hard AI based techniques such as Captcha, graphical passwords etc. have become a new area of interest. With consideration to the innovative paradigm, the most efficient and latest one is captcha, which separates and determines robotic users from actual human users by presenting a difficult challenge that can be solved with only real time human presence, i.e., a challenge as a puzzle. Most of the techniques fail in preventing shoulder surfing attacks and thereby increase the insecurity for passwords.

Right from year 1999 [3], many graphical based passwords emerged as a new technique for providing a secure way of 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. Real issues that really affect altogether, in actuality, are about convenience. GUI configuration methodologies and techniques might purposefully or accidentally influence clients' propensity or conduct towards less secure exchange practices. Hence these powerful and most secure applications must constraint high GUI related constraints based on key research work considering the abilities and shortcomings of the targeted users. In pictorial passwords, human inclination for remembering visual passwords or items will encourage the ideal choice and fitting utilization of exceedingly secure and passwords that have less consistency, shunning clients perilous practices.

LITERATURE SURVEY

The creator addresses how an assailant might infer or predict the hot-spots that are watched for utilizing in the dictionary assailant (offline). Rather than utilizing image processing technique to predict hot-spots, this framework rather uses "human computation", which depends on the people to perform different assignments that computers (at least at the current moment) find muddled to perform. Creator here process this dataset to figure out a couple sets of focuses that are more regularly and usually considered first, to generate an assault (human-seeded).

A human-seeded assault in general terms can be summarized as an assault created with the assistance of information 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 assault): two based on different styles of human-seeded assault, and another based on click-order patterns. We evaluate these dictionaries, and also combined human-seeded and click-order pattern assault, 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 assault (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.

Creator'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 client concentrate on. We explore predictive methods of generating assault 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 guess that this technique is generalizable to different sorts of graphical passwords (e.g., recognition-based) where clients are given free choice.

GRAPHICAL PASSWORDS

Graphical password is a incredible advancement and an outright different option for passwords in which clients are given a challenge to click on images to authenticate themselves rather than writing alphanumeric words which are effortlessly speculated [3]. These Graphical passwords are more memorable, as retaining images or scenes are easier than remembering complex alphanumeric length passwords, contrast to the alphanumeric passwords. Past psychological researches have experimentally and evidently proved that human brains are friendlier with memorizing images or video instead of blend of letters in order and numbers in an irregular manner [4]. For printed passwords, we need to first investigate the content, make out a semantic representation out of it and then recollect it as passwords, which is nearly repetitive. Therefore, using images or pictures rather than alphabets or numbers will help the client to improve the security compel as the alphanumeric corpus size is restricted because of constrained change and mixes.

However, on account of graphical password, the corpus size is boundless, 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 choose just 26 alphabets and 10 numbers printed instance of alphanumeric password.

GRAPHICAL PASSWORD METHODS

In this segment, we, the examination 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 recall than printed passwords. It is called as "Picture superiority effect" [2]. A literature and past survey of other proposed papers with respect to graphical password techniques imply that the techniques can be grouped or classified into groups as follows (Fig.1):

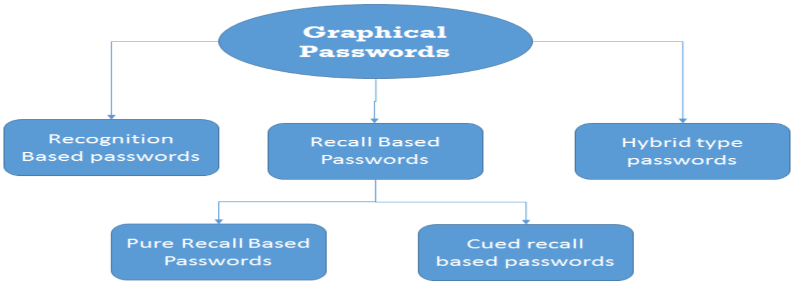
Graphical Passwords
Recognition Based passwords
Recall Based Passwords
Hybrid type passwords
Pure Recall Based Passwords
Cued recall based passwords

Figure 1: Types of graphical passwords.

RECOGNITION BASED PASSWORDS:

In this category, during registering to the system, clients need to choose images, icons or symbols from a collection of images. At the time of authentication, the clients need to perceive their images, symbols or icons which are selected at the time of enrolment among an arrangement of images. Researches were done to find the memorability of these passwords and it shows that the clients can recollect their passwords even following 45 days [4].

PURE RECALL-BASED TECHNIQUE:

With this classification, clients attempting to login to the system has to recreate their login passwords without being provided any sort of hints or update. Despite the fact that this very category is simple and convenient way, yet it strengths clients to retain the passwords that users can hardly remember. Yet it's relatively more secure than the acknowledgment based system.

CUED RECALL-BASED TECHNIQUE:

With this classification, clients are facilitated with the help of update or clues for login passwords. Such Reminders aid the clients in duplicating their login passwords or help clients to quickly remember the passwords through the insight. This worldview is entirely like the review based systems however it is review alongside prompting.

HYBRID SCHEMAS:

With this classification, the client's login authentication will be for the most part the blend of complex mix of two or more styles. Such combinational schemes are mostly used to beat the silly drawbacks of a single schemes, such as shoulder surfing, spyware and so on.

ONE TIME PASSWORD SECURITY MEASURE:

A one-time password (OTP)[6] is a password as the name recommends that is valid for verification of only one login session or exchange with the system. OTPs avoid a various confinements or shortcomings that are connected with alphanumeric traditional and usually used (static) passwords. The significant constraint or shortcoming that is seen or overcome by OTPs is, in contrast to usually used alphanumeric static passwords, they are not vulnerable or prone to replay assaults. That means even a potential gate crasher 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 exchange will not be able to forge it, since it will be no longer valid for exchange. On the other side, OTPs are additionally very troublesome for us to memorize for longer time. Therefore they require extra innovation to work. How to produce OTP and disperse to the particular user? OTP era and distribution algorithms generally make use of pseudo randomness or randomness.

This is vital on the grounds because if we don't do so, it would be very simple and easy to foresee future created OTPs by observing and analysing the past ones. Concrete and random OTP algorithms vary greatly in their workings. There are additionally different mediums or ways to make the user aware of the next OTP to use. Some OTP era systems [7] use special equipment or electronic security tokens which clients carries and then these systems produce OTPs and show it using a small LCD display.

Other OTP Generation systems consist 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 enduring 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 scientific properties cannot be manufactured.

The best example of this safe way is the one-time password algorithm (OTP)[7], where every plain text bit has a relating and proportionate key bit. One-time passwords or OTPs depend on the capability to produce the genuine new and very unique random sequence of key bits. A beast power assault would gradually reveal the actual decoding, and also all the other possible combinations of bits, and would have no chance to get of separating one from another.

A very small, i.e. 100-byte, one-time-password encoded string considered for a brute force assault would literally reveal every 100-byte string possible, including the genuine OTP as an answer, but with least probability. Here the investigation 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 assault over the one-time password algorithms have studied.

In the current (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 utilization 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 entire 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 customer application can executes a request to register with both the server and the service provider utilizing server system for generating OTP and client validation. Post fruitful execution of user activation request, the user can run the authentication request in future for a boundless number of times.

PERVASIVE CUED CLICK POINTS:

Existing graphical systems have clearly showed that image hotspots are more inclined to be speculated, which leads to very less secure image or graphical passwords and thereby increase the security rupture using dictionary attacks [10]. The study figured out whether the 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.

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.