Simple Text Based Shoulder Surfing Resistant Graphical Password Using CAPTCHA

Suvarna Jondhale[1], Shital Gunjal[2], Swati Gosavi[3], Vidya Dighe[4]

[1] *BE, Computer Engineering, Amrutvahini College Of Engineering,Sangamner, Maharashtra,, India*
[2] *BE, Computer Engineering, Amrutvahini College Of Engineering,Sangamner, Maharashtra,, India*
[3]*BE, Computer Engineering, Amrutvahini College Of Engineering,Sangamner, Maharashtra,, India*
[4] *BE, Computer Engineering, Amrutvahini College Of Engineering,Sangamner, Maharashtra,, India*

ABSTRACT

A Lot of security primitives are depend on more challenges and it will be resolved by some mathematical formulations. For security using high AI Problems and it's become an evaluation for new pattern of security, but not explored well. In our studies we define Captcha as graphically password, graphically password system build on captcha technology mainly on hard AI problems we will present new security primitives. Captcha is combination of captcha and graphical password. CaRP is address multiple security issue like shoulder surfing attack, if combined with dual view technology, relay attack and online guessing attack. 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. For improving online security highly secure password offers usability and reasonable security and appears suit well with practical applications.

Keyword : *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 [17],it was exciting new pattern. Captcha is invented for the security and it was most used technique, i.e., a puzzle. Most of another techniques are not able to keep security toward shoulder surfing attack and therefore makes the system vulnerable to attacks and however create password is insecure. In 1999 as alternative many graphical password techniques are used. 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. 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. User trying for the unsecure copying strategy, with text and credential password, like use of same password for different transaction of account to remain remember password and for avoid to remember different password for different transaction for different account, change in security level alone cannot addressed by 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. However most secure application must contain high GUI constrain base on the valid research work considered the capabilities of the targeted users. Human tendency is for remember password visual password in pictorial password or objects will facilitate the optimal selection and appropriate use of the password and password will be used having very less predictability avoid users from unsafe practice.

2. LITERATURE SURVEY

Author predict how to predict hot spot that observed for using dictionary attack and how attacker attack. Instead of using image processing technique to predict hot-spots, this systemrather 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).

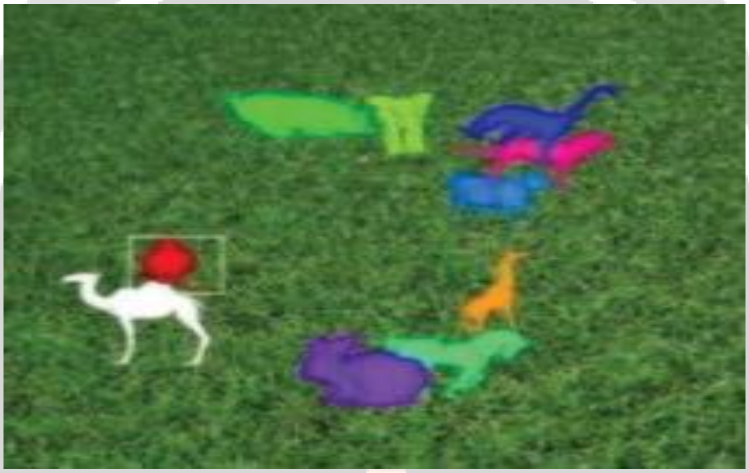


Fig.1 Use Image as graphical Password

Attack will be produce by collected data from the user a human seeded attack has been summarized in general terms. Author generates three various predictive pictorial dictionaries (i.e., on the based on available data that relate to the users login process, collect information from the outside target password database resources as user password under attack): two types of attack one is human seeded attack and second based on click order patterns. We combine the human seed attack and click order pattern as using field data set, we define these dictionaries.

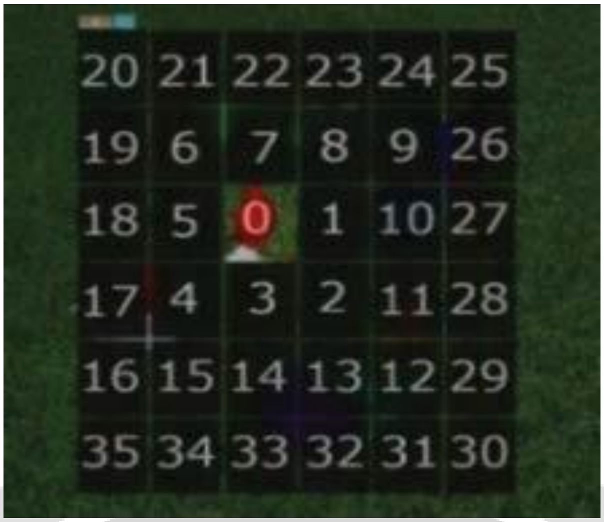


Fig.2 Captcha Zoo with horses circled red.

With our study database to train and test on human seeded attack also we define 10-fold cross validation analysis which is based on marcov model, provide information how the attacker attacks with the help these method ideal and used human computed dataset. In our studies we focus on hot spot in click based graphical password, and hoe impact on the securities. We define attack dictionary for the click based graphical password. In our studies we proposed and explored the use of human computation to generate graphical dictionary. We define that this method is suitable rather that other types of graphical password where user can having free choices.

3. GRAPHICAL PASSWORD

The alternative for the alphanumeric password the best innovation is graphical password in that user given challenge to access them by click on images instead of type alphanumeric password [3]. Alphanumeric password is lengthy password hence hard to memorized instead of graphical password is easy to memorized and easy to use as compare with alphanumeric password. As psychological experimental and evidently proved that human brains are friendlier with easy to remember images or video instead of alphanumeric password in a random fashion [4]. In alphanumeric password need to arrange proper then memorized password which is tedious. In Graphical password using images and pictures is provide more secure constrain to the password as using text and numbers

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” [13]. 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):

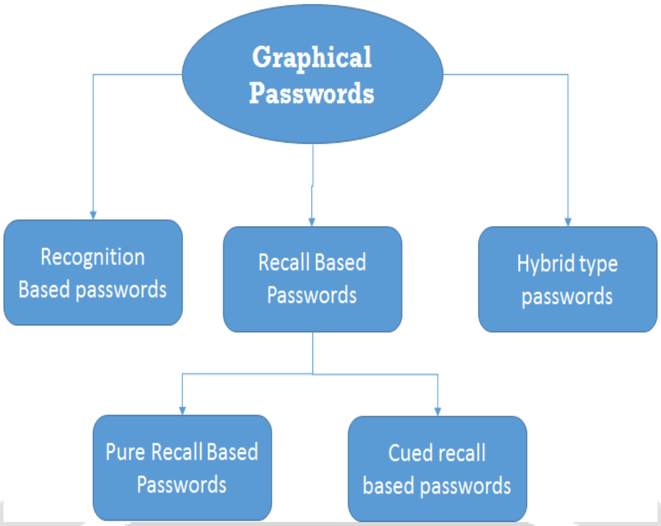

Graphical Passwords
Recognition Based passwords
Recall Based Passwords
Hybrid type passwords
Pure Recall Based Passwords
Cued recall based passwords

Fig 3 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.

B. Pure Recall-Based Technique:
With this category, users trying to login to the systemhas 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

For the valid authentication the one time password has been generated as the use for valid login which is help for password security. OPT can help for the overcome limitation. The OTP help for the valid authentication but there is possibilities intruder can able to access OTP which is previously used to login or to conduct a transaction will not be able to forge it, since it will be no longer valid for transaction. To remember OTP password id quit difficult.

Therefore they require additional technology to work. How to generate OTP and distribute to the particular use OTP generation and distribution algorithms generally make use of pseudo randomness .It would be very simple to analysis OTP as compare to previous OTP. There are chances to getting OTP as analyses previous OTPs. In some system OTP will be generated by using application and show it using a small LCD display. Other OTP Generation systems consist of some kind of software that runs on the users or clients mobile phone.

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), 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 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.

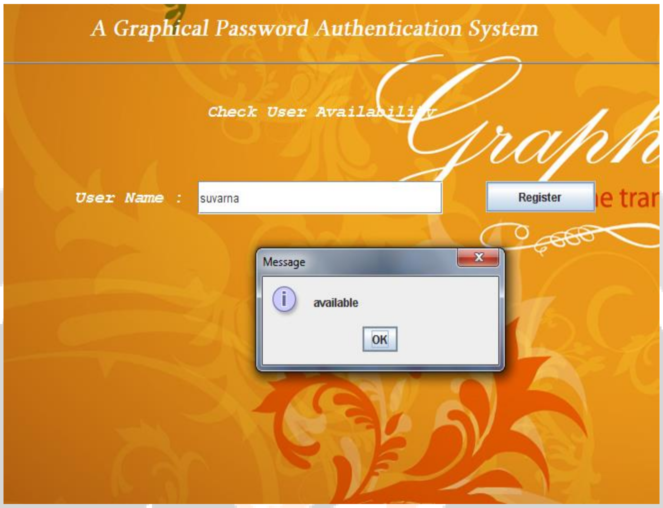
In the existing (OTP) one-time password algorithm, java Mobile midlet is a client application and we further assume that the client application runs in client's mobile phones/cellphones which will be able to receive one time passwords during login requests. A MIDlet is a java based application that makes 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. 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.

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. EXPERIMENTAL RESULT



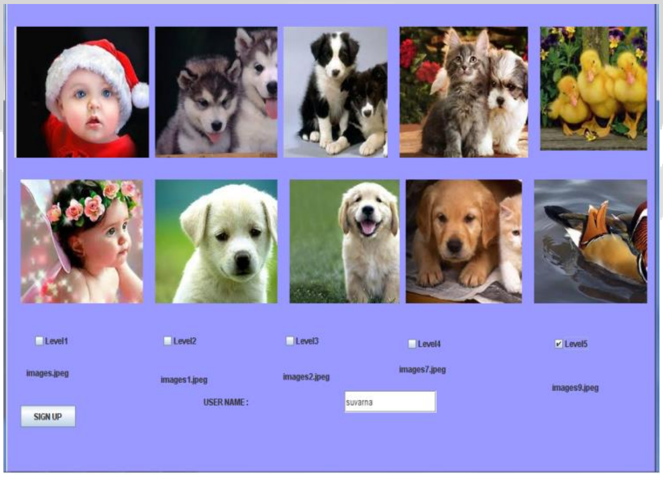
User Name : suvarna

Message

available

Fig.4 Checking Availability of User Name

Check the user mane is already available or not to register unique user name.

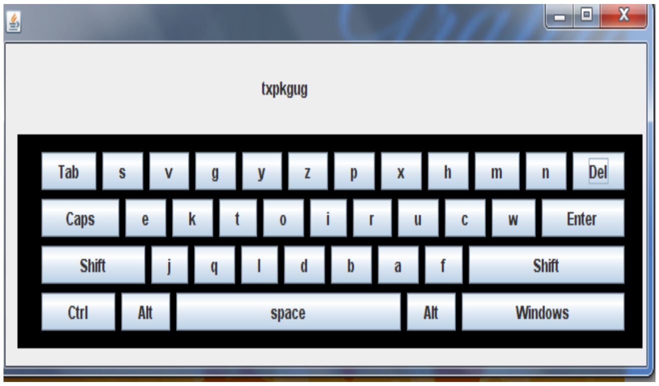


☑ Level5

USER NAME : suvarna

Fig.5 Selecting image of captcha

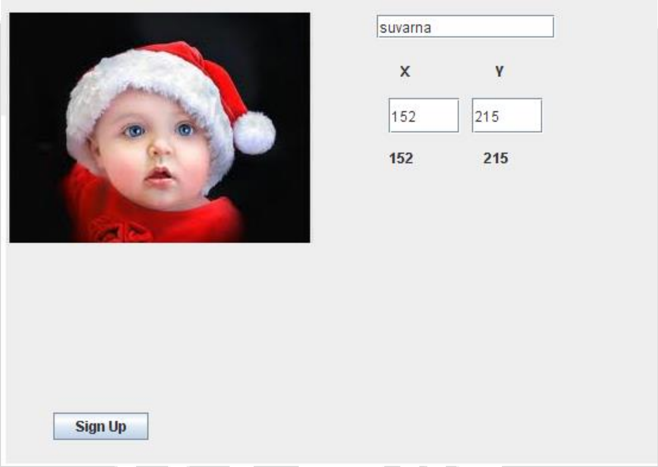
Selecting one of the image for the graphical password.



txpkgug

Fig.6 Virtual keyboard for the login

Here to prevent the shoulder surfing attack user can use virtual keyboard to enter the password.



suvarna

X Y

152 215

152 215

Fig.7 Click Point

In which clued click point saved as graphical password.

8. 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.

9. REFERENCES

[1] 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.

[2] (2012,Feb.).The Science Science Behind Passfaces [Online]. Available:http://www.realuser.com/published/ScienceBehindPassfaces.pdf

[3] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proc. 8th USENIX Security Symp., 1999, pp. 1–15.

[4] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292,2008.

[5] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon,"PassPoints: Design and longitudinal evaluation of a graphical password system," Int. J. HCI, vol. 63, pp. 102–127, Jul. 2005.

[6] P. C. van Oorschot and J. Thorpe, "On predictive models and userdrawn graphical passwords," ACM Trans. Inf. Syst. Security, vol. 10, no. 4, pp. 1–33, 2008.

[7] K. Golofit, "Click passwords under investigation," in Proc. ESORICS, 2007, pp. 343–358.

[8] A. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in Proc. Symp. Usable Privacy Security, 2007, pp. 20–28.

[9] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot spots in graphical passwords," in Proc. USENIX Security, 2007, pp. 103–118.

[10] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on passpoints-style graphical passwords," IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 393–405, Sep. 2010