New Security Primitive using Captcha as Graphical Password Against Spyware

Pallavi S. Sonar1 Pooja H. Nerkar2 Rutuja S. Aher3 Rashmila S. Pagare4 Prof. S. S. Rajebhosale5

1,2,3,4Department of Information Technology

Abstract— Today's world is based on security primitive. A key area of security is authentication, the determination of whether a user have the access to the system or not. In the past era many of the authentication method can be introduced, but the most common and convenient method for the authentication is traditional alphanumeric password. For security reason the development of graphical passwords as an alternative. They overcome the drawback of traditional password but remains vulnerable to spyware attack. It propose a graphical password scheme by using CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart). Spyware is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge. Password collection by spyware is increased. I

I. INTRODUCTION

Today's world is based on security primitive.[1] A key area in security is the authentication, the determination of whether a user have the access to the system or not. In the past era many of the authentication method can be introduced, but the most common and convenient method for the authentication uses traditional alphanumeric password. For security reason the development of graphical passwords scheme is best than the traditional alphanumeric password. They overcome or solve the limitations of traditional password scheme but it vulnerable to the spyware attack. That means it can not be resist to spyware attack. Spyware is software that main objective is to gather or collect the information about a person or organization which want to protect their confidential data without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.

Password collection by spyware is increased. In a practically spyware are continues problem. So we propose New scheme using CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart). We will use the text as well as image as password to this system based on CAPTCHA. Because of this, attacker will not able to identify the password easily. We will implement this system against spyware attack. This system will retaining the advantages of graphical password scheme.

The key area of this project is the better security. This project will protect the system from specific types of attack. We provide the images with their corresponding CAPTCHA as the security of the system. Selection of three images as pass-object from the given grid with respective to position of CAPTCHA for providing the security against the spyware. CAPTCHA is used to recognize whether the user

II. RELATED WORKS

Currently most of the present password schemes, such as [2, 4, 6, 9, 10], requires users to by enter the password directly or by clicking or drawing particular pattern. Hence, password is easily exposed to the third party. They can get the chance of getting the password successfully. The security and usability problem intrinsic in text-based password scheme which leads to development of graphical password scheme. But currently most of the presented graphical password scheme are not able to resist the spyware, which gets the control over computer without the ostentation of consumer.

In 2000 R. Dhamija, and A. Perrig. Dj Vu: A User Study Using Images for Authentication. In 9th USENIX Security Symposium, [2] R. Dhamija proposed a graphical authentication scheme based on the images. In their system, user selects a some number of images from a set of program generated random images. For a user to be authenticated, she or he should have to identify the previously-selected
One drawback of their system is that the server needs to store the seeds of the selected images of each user in plain text. And it is time consuming for user to select images from main database. It is secure authentication system but it requires more time.

In 2005 S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodsky, and N. Memon. Authentication using graphical passwords: Basic results. In Human-Computer Interaction International. Las Vegas[5]Many graphical password schemes, such as require users to enter the Password directly, typically by clicking or drawing. Hence, passwords are easily exposed to a third party who has the opportunity to record a successful password session. There have been a few graphical password schemes devoted to secure password.

In 2006 D. Weinshall Cognitive Authentication Schemes Safe Against Spyware. In Symposium on Security and Privacy.[3]D. Weinshall proposed and study some authentication system. They conducted a number of user study. The various studies includes picture recognition(image recognition) and object recognition. In the picture recognition study, out of a database of 20,000 images are used. A large set of images are present 100-200 images. Then the user easily get trained to recognize those set of images. After 1-2 months, users in their study were able to recognize over 80 percent of the images in the training set.

In April 2013 Varun Ambrose Thomas and Karanvir Kaur they design a Cursor CAPTCHA Captcha Mechanism using Mouse Cursor. This techniques are generate a random sequence of characters and together them[14]. In an image that is highly distorted and designed in an unrecognizable form. That means only humans can understand the characters in that embedded in the image. The user has to identify the characters and write them in the space that is provided in the system and submit it. The user is justified as a human when the characters get match with that used by server and CAPTCHA generator system. But the drawback of the system is only prevents to Optical Character Recognition attacks as their security is depend upon distortion.

In essence, all of above these schemes are many problems to avoid this or to overcome all these problems we propose a solution to that is a new security primitive using CAPTCHA as graphical password scheme against spyware. In 2013 Liming Wang, Xiuling Chang, Zhongjie Ren, Haichang Gao, Xiyang Liu Software Engineering Institute Xidian University[1]. They propose a new scheme that is CAPTCHA as graphical password scheme. In this scheme we present a new scheme to protect users password against spyware attack. In this system the advantage is we uses graphical password scheme. This system is based on passed image object. It improves efficiency and it also resist many kind of attacks specially spyware attack.

III. PROJECT SCHEME

This scheme is motivated by the different observations in that spyware attacks is launched by automated programs. The authentication is the main concern in security point. By analyzing all the different things we realized a scheme which is difficult for the machine by using CAPTCHA to graphical password scheme.

CAPTCHA is one kind of program designed to test whether the user is a computer or a human, it creates a task easy for humans but difficult for machines [12]. It is based on hard AI problems. CAPTCHA is almost a standard security mechanism for addressing undesirable or malicious Internet bot programs [11] and web sites such as Google, Yahoo and Microsoft all have their own CAPTCHAs. The CAPTCHAs mainly include three types: text-based schemes, sound-based schemes and image-based schemes. The most widely deployed schemes are text-based CAPTCHAs and we also use this in this schemes.

The basic system can provide a grid of images with the corresponding conjugative string. That string is collection of CAPTCHA which is automatically generated by the system. At registration phase user want to select and remember set of 3 images as a password and provide the position for the conjugative string and at the login time user want to enter the CAPTCHA with the corresponding position which is stored at the time of registration.

In the previous scheme the CAPTCHA can be generated with using only small alphabets but for increasing complexity to spyware we can generate the CAPTCHA as a collection of alphabets in which small as well as capital and also the special symbols and numbers. Also the security can be increased by providing 3 different kinds of dataset which includes the images of flowers, natures and cartoon. As per the user selected dataset the images can be display to the user at the time of login and user just want to enter the CAPTCHA of the corresponding position with respective images.

For the simplicity, we generate the CAPTCHA here is an ideal CAPTCHA that is enough hard for the machines to recognize but easy for the humans to solve same kind. In this scheme the reversible relationship present between the password and what is to be entered. That is, pass-images determine what is entered and vice-versa. In that system every time the new password is generated that corresponding to the pass-images as well as the pass-positions. The user’s entered CAPTCHA is changed with every new login. Hence, every time the new password is generated.

In the case of automated programs without human intervention, the scheme can strongly resist to the replay attack. After, even if observing a successful login, a spyware program cannot lunch a replay attack. There are many kinds of attacks such as shoulder surfing, spammer attack, phishing, can be avoided in this scheme that can be seen as reference to the this improved scheme.

As shown in figure 1 user want to select the three images from grid of images. It is the process at the time of registration. The images selected by the user are checked as shown in fig. The images selected by the user are shown by the check boxes. There are 3 types of dataset is used that is the cartoon, nature and flowers as per user selection it can be represent to the user.
The next step after the selection of images is to decide the sequence of images. User can change the sequence if the images as per his/her requirement. And finally the user are select and remember the letters position. These letter position is called as pass-position.

After the successful registration user want to enter login to the system by providing appropriate username the dataset selected by the user are display to the user. User just want to enter the corresponding CAPTCHA of the selected images with appropriate pass-position which is only known to the user. In Figure 2, the three pass-images, the strings with them are ‘BO@qLP’, ‘MNM!5B’, and ‘HpbDhX’ respectively, and the corresponding pass-positions are (2, 4, 6), (4, 5, 5), and (4, 5, 6) shown in Figure 2. A user can input combination of the three sequences, ‘OqP’, ‘!55’, and ‘DhX’ to be authenticated successfully. The space provided for the password user want to enter the corresponding CAPTCHA. After entering right CAPTCHA user can successfully login to the system.

This system will be develop for the better security which prevent the system from specific types of attack. Also now-a-days, users require the passwords for their personal computers, social networks, email and more and to websites which needs the better security.

To remember the password easily the users can use the same password which reduces security. Because of this the attacker can be easily attack the system. So in this way if textual passwords are kept difficult then they are difficult to remember but it may be hacked by the attacker and if it kept as easy then they are easy to guess which reduces the security. Only use of the text as a password will not be sufficient for user. For that we have to use some images. So alternative scheme to textual password, is the graphical password scheme. Mainly it is focuses on spyware attack.

In this system, the database is used to store the images and the text-based CAPTCHA. In this system we will use some images and text with their corresponding CAPTCHA which is send by the system for user authentication. The system will give the images and text-based CAPTCHA which will be collect or gather from the databases.
The server is shown in system. That server consist of the two server that is the web server and database server. Database server is used for fetching some images and text-based CAPTCHA from the database. Database contains the huge amount of images and text-based CAPTCHA. So the database server will fetch only those images and text-based CAPTCHA which is going to available to the user for their registration after that for the users authentication. That images and the text-based CAPTCHA will change their position at the time of the user login. This will used for the authentication of user and due to this the security of system will gets increase. Through the web server that images and text-based CAPTCHA will be shown to the user for proceeding the registration and login process of the users. User can authenticate it by using authentication process.

B. Working Module

This scheme can be introduced better security. As per the convenience this system can be divide into three parts. That are include the development of web-based project.

IV. IMPLEMENTATION DETAILS

A. Algorithm

1) Captcha Generation Algorithm

Input : Set of characters  
Set of images  
Set of font  
Set of colors  
Output : CAPTCHA image  
Processing :  
for 1 to 50(for each grid) 
select random character  
(i=0 to 10)
for each character  
select and apply random font  
select and apply random color  
select and apply random transition  
select and apply random rotation  
select and apply random skewness  
select and apply random blur  
add character to string  
end for

Fig. 4: Work Breakdown Structure

The project can in the form of static and dynamic. The static part can be used for some part of this system that can't be changes i.e. the overview. The dynamic part can be include generation of CAPTCHA and change position of images. That can be change every time of login. As we know generation of CAPTCHA is important so we generate the text-based CAPTCHA and images with corresponding CAPTCHA. Finally the authentication phase that include the both the image with the corresponding CAPTCHA positions.

B. Analysis

In comparison of different graphical password schemes, such as [2, 5, 13], there are some advantages and also the disadvantages in this scheme. One of the disadvantage is that is increase the users memory load. It is necessary for the user to remember pass-images as well as the pass-position. for the successful authentication user need to remember the
images with sequence of the images and enter the appropriate input the text-based CAPTCHA of the corresponding image pass-position. All this factors increase the login time. And complexity of login process, but this scheme resist the spyware attack which is this primary focus.

As compared with the other text based scheme the login time of this system is longer but comparison with other graphical schemes this login time is shorter. Such as[3,5].

There are some of strong advantages of this system like antiphishing[15]. This added some extra pages at the start to system in order to prevent attack like the attacker can take the snapshots of system and try to make a same system. Other is that the backend of this system is MongoDB which already secure as well as it can stores the huge amount of data in database. In that the encryption is apply on the users data within database and only the authenticate user can decrypt their own data.

In this system, the different kinds of symbols are included with the upper case letters and very few number of small letters. Which also useful for system as well as authenticated users.

VI. SNAPSHOT
In this topic the look up of the project can be shown. The first page of the system shown below in Figure 3. It shows the options such as SIGN IN and SIGN UP for login and registration. This system is mainly focused on the security. So, this page is worked for the phishing. The phishing attacks can be prevented due to this.

![First page](image)

**Fig. 5: First page**

For the new user it is necessary to first register to the system as shown in Figure 4. Then next the registration page is opened after clicking on SIGN UP. All fields are required to be filled by user. The field Password images contains the dataset as per user want the dataset is display to the user and further processing takes place as shown in figure 1 a and 2.

![Registration page](image)

**Fig. 6: Registration page**

The cartoon dataset is shown in figure 1 and 2 at the login and registration process. If the user select the password images as Flowers or the Nature the that specific kind of images are display to the user as shown in figure 7 (a) and (b). As per the user selection the dataset i.e. the password images are display to the user at the time of login.

![Password Images](image)

**Fig. 7: Password Images(Dataset)**

VII. CONCLUSION
In this project, we have shown a new approach to protect users password which resist to spyware attack. The main work of this system is that to introduce CAPTCHA as a
graphical passwords scheme which resist to spyware programs. From a security perspective, this project is about to doing the advance and enhance development of graphical passwords scheme. At the time of design of CAPTCHA, we do not say you that this scheme is immediately feasible. However, we believe and assure you that this method will enhance current security and as we using the CAPTCHA in this system, so it will increases effectiveness in this method and this will increase computer security too.

REFERENCES

[1] "Liming Wang, Xiuling Chang, Zhongjie Ren, Haichang Gao, Xiyang Liu Against Spyware Using CAPTCHA in Graphical Password Scheme , The University of Nottingham Nottingham, NG8 1BB, U.K. uxa@cs.nott.ac.uk 2013."