AN INTEGRATED EVADER DEFENDANT SCHEME FOR CLIENT CERTIFICATION PROCESS

S.Karthika[1], Dr.P.Devaki[2]

[1] Student, [2] Assistant Professor

Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, (India)

ABSTRACT

Graphical passwords are knowledge-based authentication mechanisms where users enter a shared secret as evidence of their identity. Graphical passwords are composed with images and sketches with human memory for visual information. Improved password memorability and strength against guessing attacks are the key benefits of graphical password schemes. Captcha as graphical passwords (CaRP) is a graphical password scheme used for user authentication. CaRP is click-based graphical password where a sequence of clicks on an image is used to derive a password. Dynamic captcha challenge image is used for each login attempt in CaRP. Text Captcha and image-recognition Captcha are used in CaRP scheme. CaRP schemes can be classified into two categories as recognition based CaRP and recognition-recall based CaRP. Recognition-based CaRP seems to have access to an infinite number of different visual objects. Recognition-recall based CaRP requires recognizing an image and using the recognized objects as cues to enter a password. Recognition-recall combines the tasks of both recognition and cued-recall. Password information is transferred and verified using hash codes. Secure channels between clients and the authentication server through is Transport Layer Security (TLS). The CaRP scheme is enhanced with strength analysis and security features.

Keywords: Captcha, Cortcha, Graphical Password, IRC, TLS

I. INTRODUCTION

Security methods are required to handle unauthorized user access attempts. Security practitioners and researchers have made strides in protecting systems and, correspondingly, individual users' digital assets. The problem arises that, until recently, security was treated wholly as a technical problem – the system user was not factored into the equation. Users interact with security technologies either passively or actively [1]. For passive use understandability may be sufficient for users. For active use people need much more from their security solutions: ease of use, memorability, efficiency, effectiveness and satisfaction. Today there is an increasing recognition that security issues are also fundamentally human-computer interaction issues. Authentication is the process of determining whether a user should be allowed access to a particular system or resource. It is a critical area of security research and practice. Alphanumeric passwords are used widely for authentication, but other methods are also available today, including biometrics and smart cards. There are problems of these alternative technologies. Biometrics raise privacy concerns and smart cards usually need a PIN because cards can be lost. As a result, passwords are still dominant and are expected to continue to remain so for some time. Yet traditional alphanumeric passwords have drawbacks from a usability standpoint and these usability problems tend to translate directly into security problems. That is, users who fail to choose and handle passwords securely open holes that attackers can exploit. The "password problem," as formulated by Birget, arises because passwords are expected to comply with two conflicting requirements, namely:

1. Passwords should be easy to remember and the user authentication protocol should be executable quickly and easily by humans.
2. Meeting these conflicting requirements is almost impossible for humans, with the result that users compensate by creating weak passwords and handling them in an insecure way.

Many problems that users have with alphanumeric passwords are related to memorability of secure passwords. In an attempt to create more memorable passwords, graphical password systems have been devised. In these systems authentication is based on clicking on images rather than typing alphanumeric strings. Several kinds of graphical passwords have been invented. In this paper a new kind of graphical password system, called PassPoints and have done studies of its human factors characteristics compared to alphanumeric password. This paper also report on further research on usability and memorability of our system under different conditions. In specific this paper investigate the effect of the tolerance, or the margin of error, allowed when entering one's password points and the effect of the choice of images used in the password system.

Various graphical password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown that text-based passwords are fraught with both usability and security problems that make them less than desirable solutions [2]. Psychology studies have revealed that the human brain is better at recognizing and recalling images than text; graphical passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to cope.

II. BACKGROUND AND RELATED WORK

Most current graphical password schemes, 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 authentication session. There have been a few graphical password schemes devoted to secure passwords against spyware attacks. In the following, several representatives will be described. Man, et al proposed that users remember a number of text strings as well as several images as pass-objects. To pass the authentication, users should enter the unique codes corresponding to the displayed pass-object variants and a code indicating the relative location of the pass-objects in reference to a pair of eyes. It is relatively hard to crack this kind of password, but the complex memory requirement is an obstacle to its popularity.

In [6], users need to recognize pass-objects and click inside the convex hull formed by all of the pass-objects. If properly designed, this method can provide good security. From time to time the convex hull is either too small to click or too large, creating a guessing problem. Moreover, to provide a large password space may result in a crowed screen and indistinguishable objects. The method to resist shoulder-surfing is a trivial trick, where a user must click a group composed of both the pass-object and decoy-object rather than click the pass-objects directly. The prototype presented does not provide sufficient security, having only two objects in each group.

In 2006, Weinshall proposed another challenge-response protocol that relied on a shared secret set of pictures [8]. To reduce the amount of information given out with each authentication session, the image set memberships are used to select a certain path on an image mosaic, with the user providing only a code that depends on the path's endpoint. This scheme was claimed to be so strong that an observer who fully records any feasible series of successful interactions could not compute the user's password. It was demonstrated by Golle and Wagner [9] that the attacker can learn a user's secret key with a SAT solver after observing as few as six successful user logins. In essence, the above methods adopt a challenge-response protocol to confuse the spyware. They can prevent the passwords being cracked by the spyware and falling into the hand of an adversary, along with resisting replay attacks. Taking the previous mechanisms for reference, our scheme also uses a challenge-response protocol to enhance security. But, unlike these methods, our scheme innovatively applies CAPTCHA to graphical passwords to create a highly secure authentication method.

III. EXISTING WORK

3.1 Captcha as Graphical Passwords (CaRP)

In CaRP, a new image is generated for every login attempt, even for the same user. CaRP uses an alphabet of visual objects to generate a CaRP image, which is also a Captcha challenge. A major difference between CaRP images and Captcha images is that all the visual objects in the alphabet should appear in a CaRP image to allow a user to input any password but not necessarily in a Captcha image. CaRP schemes are clicked-based graphical passwords. According to the memory tasks in memorizing and entering a password, CaRP schemes can be classified into two categories: recognition and a new category, recognition-recall, which requires recognizing an image and using the recognized objects as cues to enter a password [7]. Recognition-recall combines the tasks of both recognition and cued-recall and retains both the recognition-based advantage of being easy for human memory and the cued-recall advantage of a large password space. Exemplary CaRP schemes of each type will be presented later.

In principle, any visual Captcha scheme relying on recognizing two or more predefined types of objects can be converted to a CaRP. All text Captcha schemes and most IRCs meet this requirement [3]. Those IRCs that rely on recognizing a single predefined type of objects can also be converted to CaRPs in general by adding more types of objects. In practice, conversion of a specific Captcha scheme to a CaRP scheme typically requires a case by case study, in order to ensure both security and usability. We will present several CaRPs built on top of text and image-recognition Captcha schemes. Some IRCs rely on identifying objects whose types are not predefined. A typical example is Cortcha which relies on context-based object recognition wherein the object to be recognized can be of any type. These IRCs cannot be converted into CaRP since a set of pre-defined object types is essential for constructing a password.

Like other graphical passwords, we assume that CaRP schemes are used with additional protection such as secure channels between clients and the authentication server through Transport Layer Security (TLS). A typical way to apply CaRP schemes in user authentication is as follows [10]. The authentication server AS stores a salt s and a hash value H(ρ, s) for each user ID, where ρ is the password of the account and not stored. A CaRP password is a sequence of visual object IDs or clickable-points of visual objects that the user selects. Upon receiving a login request, AS generates a CaRP image, records the locations of the objects in the image, and sends the image to the user to click her password. The coordinates of the clicked points are recorded and sent to the user ID. AS maps the received coordinates onto the CaRP image, and recovers a sequence of visual object IDs or clickable points of visual objects, ρ, that the user clicked on the image. Then AS retrieves salt s of the account, calculates the hash value of ρ' with the salt, and compares the result with the hash value stored for the account. Authentication succeeds only if the two hash values match. This process is called the basic CaRP authentication.

Advanced authentication with CaRP challenge-response will be presented. We assume in the following that CaRP is used with the basic CaRP authentication unless explicitly stated otherwise. To recover a password successfully, each user-clicked point must belong to a single object or a clickable-point of an object. Objects in a CaRP image may overlap slightly with neighboring objects to resist segmentation. Users should not click inside an overlapping region to avoid ambiguity in identifying the clicked object. This is not a usability concern in practice since overlapping areas generally take a tiny portion of an object.

IV. PROPOSED WORK

The CaRP scheme is enhanced with strength analysis and security features. Pattern based attacks are handled with Color and Spatial patterns. Pixel colors in click points are considered in the color pattern analysis model. Pixel location patterns are considered in the spatial pattern analysis model. Dictionary attacks and transmission attacks handling process is also improved with high security. Password security level assessment mechanism is used in the graphical password construction process. Cryptography (RSA) and data integrity (SHA) schemes are also integrated with the system to improve the security level in online applications. CAPTCHA and graphical password schemes are used for the user authentication process. Pixel physical and spatial properties are used in the strength analysis process. Transmission security is improved with integrity verification mechanisms.

The system is divided into six major modules. They are CaRP with Text CAPTCHA, authentication server, CaRP with image Recognition CAPTCHA, pattern analysis, attack handler and enhanced CaRP scheme. Character sequence selection is used in CaRP with Text CAPTCHA scheme. The authentication server is designed to manage and verify the user accounts. CaRP with Image Recognition CAPTCHA scheme uses the recognition and recall mechanism with image objects. The color and spatial patterns are analyzed under the pattern analysis module. The directory and shoulder surfing attacks are handled under attack handler module. Enhanced CaRP Scheme integrates the security and attack control mechanism for user authentication process.

4.1 Working

4.1.1 CaRP with Text Captcha

Textual characters based CAPTCHA is used in Text CaRP scheme. Password is constructed by selecting character sequences in the text CAPTCHA collection. The textual CAPCHA characters are dynamically rearranged at the time of recognition process. Password details are converted into hash codes and applied in verification process.

4.1.2 Authentication Server

The authentication server application is used to authenticate the users. User registration and password management operations are carried out under the server. Password verification is carried out under the server. Key and signature values are maintained under the server.

4.1.3 CaRP with Image Recognition Captcha

Image objects are used in recognition-recall based CaRP Recognition CAPTCHA. Object recognition and click cue identification mechanism are used in the system. Rectangular regions are used in the cued recall process. CAPTCHA-Zoo image object collection is used for the password construction process.

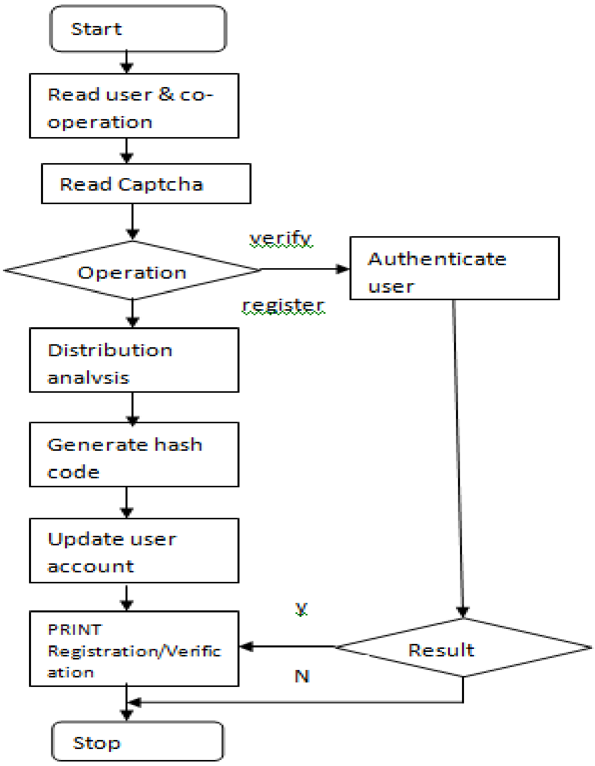

Fig. No: 1.1 Integrated Evader Defendant Scheme for Client Certification

4.1.4 Pattern Analysis

Color and spatial patterns are analyzed in the system. Pixel color for click points are used in the color pattern analysis. Spatial patterns are extracted from location information. Password complexity is assessed with pattern information.

4.1.5 Attack Handler

Directory and shoulder surfing attacks are managed by the system. RSA algorithm is used to perform password encryption/decryption tasks. Image dimming mechanism is used to control shoulder surfing attacks. Mouse cursor size and location are automatically adjusted for attack handling process.

4.1.6 Enhanced CaRP Scheme

CaRP scheme and attack handling mechanism are integrated in the Enhanced CaRP scheme. Distribution, strength and pattern analysis schemes are integrated with CaRP scheme. The Secure hashing algorithm (SHA) is used to generate password signatures. Reusability level is analyzed.

V. CONCLUSION

The graphical passwords are used to ensure the high level security for the remote logins. CAPTCHA techniques are used to verify the source type of request. Captcha as Graphical Passwords scheme integrates the text and image captchas to construct graphical password scheme. CaRP scheme is enhanced with strength based password construction and attack resistant user authentication model. Password complexity prediction system is integrated to improve password construction process. The system increases the success and recall rates. User interface is upgraded to avoid capture attacks in password recall process. Efficient shoulder surfing attack controlling models are used to protect the system from attackers.

REFERENCES

[1] S. Wiedenbeck and Memon, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," Proc. First Symp. Usable Privacy and Security, July 2005.

[2] S. Chiasson, P. van Oorschot and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security, 2007.

[3] HP TippingPoint DVLabs, Vienna, Austria. Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs [Online]. Available: http://dvlabs.tippingpoint.com/toprisks 2010.

[4] Mun-Kyu Lee, "Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry", IEEE Transactions On Information Forensics And Security, April 2014

[5] N.Joshi.Koobface Worm Asks for CAPTCHA [Online]. Available:http://blogs.mcafee.com/mcafee-labs/koobface-worm-asksfor- CAPTCHA, 2009

[6] S. Wiedenbeck. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In Proceedings of the Working Conference on Advanced Visual Interface, New York, NY : ACM Press, 2006. pp. 177-184.

[7] Napa Sae-Bae and Kowsar Ahmed, "Multitouch Gesture-Based Authentication" IEEE Transactions On Information Forensics And Security, Vol. 9, No. 4, April 2014

[8] D. Weinshall. Cognitive Authentication Schemes Safe Against Spyware. In Symposium on Security and Privacy, 2006.

[9] P. Golle and D.Wagner. Cryptanalysis of a Cognitive Authentication Scheme. In Symposium on Security and Privacy, 2007.

[10] Sooyeon Shin and Sarang Na, "Covert Attentional Shoulder Surfing: Human Adversaries Are More Powerful Than Expected", IEEE Transactions On Systems, Man, And Cybernetics: Systems, June 2014.

[11] Bin B. Zhu, Jeff Yan, Maowei Yang and Ning Xu, "Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems" IEEE Transactions On Information Forensics And Security, Vol. 9, No. 6, June 2014.

[12] Xiaoyuan Suo ,Ying Zhu, G. Scott. Owen "Graphical Passwords: A Survey" in Computer world, May 10, 2006.

[13] Ved Prakash Singh, Preet Pal "Survey of Different Types of CAPTCHA" International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2242-2245.

[14] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in *Proc. ACM CCS*, 2002, pp. 161–170.

[15] P. C. van Oorschot and S. Stubblebine, "On countering online dictionary attacks with login histories and humans-in-the-loop," *ACM Trans. Inf. Syst. Security*, vol. 9, no. 3, pp. 235–258, 2006.