www.ijiarec.com

ISSN: 2348-2079

MAY-2015

International Journal of Intellectual Advancements and Research in Engineering Computations

AN EFFICIENT CLIENT AUTHENTICATION MECHANISM FOR REMOTE SERVICE PROVIDERS

[1]B. Yugadharini, [2]S. Lalithambikai

ABSTRACT

Images and captcha are integrated to build Captcha as graphical passwords (CaRP) scheme. Online guessing attacks, relay attacks and shoulder surfing attacks are handled in CaRP. CaRP is click-based graphical passwords 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. Text CaRP scheme constructs the password by clicking the right character sequence on CaRP images. CaRP schemes can be classified into two categories 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 Transport Layer Security (TLS). The image based passwords are constructed with strength analysis mechanism. 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.

INTRODUCTION

Graphical passwords have been proposed as a useful authentication method for Personal Digital Assistants (PDAs) which are increasingly used with their small size, compact deployment and low cost. Given the fact that pictures are generally easier to remember than words and that humans are the 'weakest link' in any password authentication mechanism, it is conceivable that graphical passwords would be able to provide a good tradeoff between usability and security.

Most of the current graphical password schemes are vulnerable to shoulder-surfing, a known risk where an attacker can capture a password by direct observation or by recording the authentication session. Due to the visual interface, shoulder-surfing becomes an exacerbated problem in graphical passwords. Several approaches have been developed to deal with this problem, but they have significant usability drawbacks, usually in the time and effort to log in, making them less suitable for everyday authentication [13]. For example, it is time-consuming for users to log in CHC and there are complex text memory requirements in scheme proposed by Hong. With respect to the scheme proposed by We in shall, not only is it intricate to log in, but also the main claim of resisting shoulder-surfing is proven false. We introduce a new graphical password scheme which provides a good resistance to shoulder-surfing and preserves a desirable usability.

Our inspiration comes from two representative graphical password schemes: DAS and Story. DAS allows users to draw a free-form picture on N N × grid to produce a password and Story requires users to select a sequence of images to make a story. Our new shoulder-surfing resistant scheme CD adopts a similar drawing input method in DAS and inherits the association mnemonics in Story for sequence retrieval. It requires users to draw a curve across their password images orderly rather than click directly on them. The drawing method seems to be more compatible with people's writing habit, which may shorten the login time. The drawing passes through both pass-images and decoys, which used to

Author for Correspondence:
[1]Final year ME CSE, Mahendra Institute of Technology, Mahendhrapuri, Tamilnadu, India.
[2]Assistant Professor/CSE, Mahendra Institute of Technology, Mahendhrapuri, Tamilnadu, India.

confuse peepers. To avoid revealing the first and last pass-images, the drawing must begin and end with given random images. To enhance its shoulder-surfing resistant properties further, CDS displays degraded images which are difficult to distinguish from a distance or from a side view. Moreover, the majority of the drawing trace will be cleared away as the stylus being sliding, reducing the probability of passwords being revealed. Other complementary measures, such as limiting the length of drawing trace, are also deployed to strengthen the security.

RELATED WORK

A large number of graphical password schemes have been proposed. They can be classified into three categories according to the task involved in memorizing and entering passwords: recognition, recall and cued recall. Each type will be briefly described here. More can be found in a recent review of graphical passwords [1]. A recognition-based scheme requires identifying among decoys the visual objects belonging to a password portfolio. A typical scheme is Pass faces [2] wherein a user selects a portfolio of faces from a database in creating a password. During authentication, a panel of candidate faces is presented for the user to select the face belonging to her portfolio. This process is repeated several rounds, each round with a different panel. A successful login requires correct selection in each round. The set of images in a panel remains the same between logins, but their locations are permuted. Story is similar to Pass faces but the images in the portfolio are ordered and a user must identify her portfolio images in the correct order. Deja Vu is also similar but uses a large set of computer generated "random-art" images. Cognitive Authentication [5] requires a user to generate a path through a panel of images as follows: starting from the top-left image, moving down if the image is in her portfolio, or right otherwise. The user identifies among decoys the row or column label that the path ends. This process is repeated, each time with a different panel. A successful login requires that the cumulative probability that correct answers were not entered by chance exceeds a threshold within a given number of rounds.

A recall-based scheme requires a user to regenerate the same interaction result without cueing. Draw-A-Secret (DAS) was the first recall-based scheme proposed. A user draws her password on a 2D grid. The system encodes the sequence of grid cells along the drawing path as a user drawn password. Pass-Go [4] improves DAS's usability by encoding the grid intersection points rather than the grid cells. BDAS [6] adds background images to DAS to encourage users to create more complex passwords.

In a cued-recall scheme, an external cue is provided to help memorize and enter a password. Pass Points is a widely studied click-based cued-recall scheme wherein a user clicks a sequence of points anywhere on an image in creating a password and re-clicks the same sequence during authentication. Cued Click Points (CCP) [8] is similar to Pass Points but uses one image per click, with the next image selected by a deterministic function. Persuasive Cued Click Points (PCCP) [9] extends CCP by requiring a user to select a point inside a randomly positioned viewport when creating a password, resulting in more randomly distributed click-points in a password.

It was introduced to use both Captcha and password in a user authentication protocol, which we call Captcha-based Password Authentication (CbPA) protocol, to counter online dictionary attacks. The CbPA-protocol requires solving a Captcha challenge after inputting a valid pair of user ID and password unless a valid browser cookie is received. For an invalid pair of user ID and password, the user has a certain probability to solve a Captcha challenge before being denied access. An improved CbPA-protocol is proposed by storing cookies only on user-trusted machines and applying a Captcha challenge only when the number of failed login attempts for the account has exceeded a threshold. It is further improved by applying a small threshold for failed login attempts from unknown machines but a large threshold for failed attempts from known machines with a previous successful login within a given time frame.

CARP OPERATIONS

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. 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. 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. 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.

RECOGNITION-RECALL CARP

In recognition-recall CaRP, a password is a sequence of some invariant points of objects. An invariant point an object is a point that has a fixed relative position in different incarnations the object and thus can be uniquely identified by humans no matter how the object appears in CaRP images. To enter a password, a user must identify the objects in a CaRP image and then use the identified objects as cues to locate and click the invariant points matching her password. Each password point has a tolerance range that a click within the tolerance range is acceptable as the password point. Most people have a click variation of 3 pixels or less. Text Point, a recognition recall CaRP scheme with an alphabet of characters, is presented next, followed by a variation for challenge response authentication.

TEXTPOINTS

Characters contain invariant points. Some invariant points of letter "A", which offers a strong cue to memorize and locate its invariant points. A point is said to be an internal point of an object if its distance to the closest boundary of the object exceeds a threshold. A set of internal invariant points of

characters is selected to form a set of clickable points for Text Points. The internality ensures that a clickable point is unlikely occluded by a neighboring character and that its tolerance region unlikely overlaps with any tolerance region of a neighboring character's clickable points on the image generated by the underlying Captcha engine. In determining clickable points, the distance between any pair of clickable points in a character must exceed a threshold so that they are perceptually distinguishable and their tolerance regions do not overlap on CaRP images. In addition, variation should also be taken into consideration. For example, if the center of a stroke segment in one character is selected, we should avoid selecting the center of a similar stroke segment in another character. Instead, we should select a different point from the stroke segment, e.g., a point at one-third length of the stroke segment to an end. This variation in selecting clickable points ensures that a clickable point is context-dependent: a similarly structured point may or may not be a clickable point, depending on the character that the point lies in. Character recognition is required in locating clickable points on a Text Points image although the clickable points are known for each character. This is a task beyond a bot's capability.

TEXTPOINTS4CR

For the CaRP schemes presented up to now, the coordinates of user-clicked points are sent directly to the authentication server during authentication. For more complex protocols, say a challenge-response authentication protocol, a response is sent to the authentication server instead. Text Points can be modified to fit challenge-response authentication. This variation is called Text Points for Challenge-Response or TextPoints4CR.

Unlike Text Points wherein the authentication server stores a salt and a password hash value for each account, the server in TextPoints4CR stores the password for each account. Another difference is that each character appears only once in a TextPoints4CR image but may appear multiple times in a Text Points image. This is because both server and client in TextPoints4CR should generate the same sequence of discretized grid-cells independently. That requires a unique way to generate the sequence from the shared secret, i.e., password. Repeated characters would lead to several possible sequences for the same password. This unique sequence is used as if the shared secret in a conventional challenge response authentication protocol.

In TextPoints4CR, an image is partitioned into a fixed grid with the discretization grid-cell of size μ along both directions. The minimal distance between any pair of clickable points should be larger than μ by a margin exceeding a threshold to prevent two clickable points from falling into a single grid-cell in an image. Suppose that a guaranteed tolerance of click errors along both x-axis and y-axis is τ , we require that $\mu \geq 4\tau$.

Unlike other CaRP schemes presented in this paper, Text-Points4CR requires the authentication server to store passwords instead of their hash values. Stored passwords must be protected from insider attacks; for example, they are encrypted with a master key that only the authentication server knows. A password is decrypted only when its associated account attempts to log in.

SPYWARE AND SHOLDER SURFING ATTACKS

A key area in security research and practice is authentication, the determination of whether a user should be allowed to access to a given system or resource. Generally, the most common and convenient authentication method is the traditional alphanumeric password [11]. Their inherent security and usability problems led to the development of graphical passwords as an alternative. To date, there have been several graphical password schemes [10]. They have overcome some drawbacks of traditional password schemes, but most of the current graphical password schemes remain vulnerable to spyware attacks.

To cope with this problem, which is between the user and the system, cryptographic prevention techniques are hardly applicable because human users are limited in their capacity to process information. Instead, there have been alternative approaches considering the asymmetry between the user and the system. Among them, the PIN entry method presented by Roth *et al.* was elegant because of its simplicity and intuitiveness: in each round, a regular numeric keypad is colored at random, half of the keys in black and the other half in white, which we will call the BW method [12]. A user who knows

the correct PIN digit can answer its color by pressing the separate color key below. The basic BW method is aimed to resist a human shoulder surfing attack, not supported by a recording device, while its probabilistic extension considers a recording attack in part. The BW method is still considered to be secure against human adversaries due to the limited cognitive capabilities of humans.

PROBLEM DEFINITION

Captcha as graphical passwords (CaRP) is a graphical password scheme used for user authentication. Online guessing attacks, relay attacks and shoulder surfing attacks are handled in CaRP. CaRP is click-based graphical passwords 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. Text CaRP scheme constructs the password by clicking the right character sequence on CaRP images. CaRP schemes can be classified into two categories 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 Transport Layer Security (TLS). The following problems are identified from the current CaRP scheme.

- Click point relationship are not analyzed
- Directory attacks are not handled
- Device dependant shoulder surfing attack handling mechanism
- Hash code security is not considered

SECURITY SOLUTIONS

RSA ALGORITHM

The domain name service sensitive attributes are secured using the RSA algorithm. The Revert, Shamir, Adelman (RSA) scheme is a block cipher in which the Plaintext and cipher text are integers between 0 and n-1 for some n. A typical size for n is 1024 bits or 309 decimal digits.

KEY GENERATION

Select p,q

p and q both prime , $p \neq q$

Calculate $n = p \times q$

Calculate $\phi(n)=(p-1)(q-1)$

Select integer e

$gcd(\phi(n),e) = 1; 1 < e < \phi(n)$

Calculate d

$d = e^{-1} \bmod \phi(n)$

Public key

$KU = \{e, n\}$

Private key

$KR = \{d, n\}$

ENCRYPTION

Plaintext $M < n$

Cipher text

$C = M^e \pmod n$

DECRYPTION

Cipher text

C

Plaintext $M = C^d \pmod n$

SECURE HASHING ALGORITHM

The Secure Hash Algorithm is a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS). A 160-bit hash function which resembles the earlier MD5 algorithm. This was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm. Cryptographic weaknesses were discovered in SHA-1 and the standard was no longer approved for most cryptographic uses after 2010.

CLIENT AUTHENTICATION FOR REMOTE SERVICE PROVIDERS

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.

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.

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.

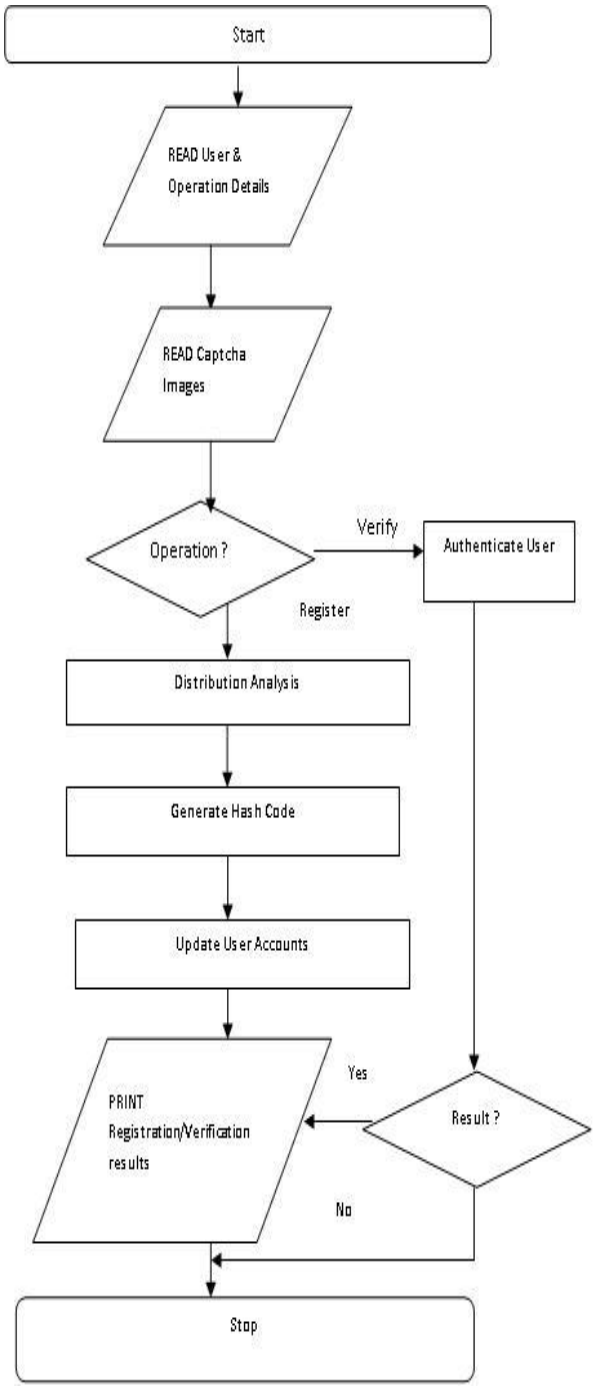

Fig. No: 8.1. Client Control Management using Images

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.

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.

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.

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.

CONCLUSION

The client control management scheme uses the images for verification process in remote access environment. 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]. R. Biddle, S. Chiasson and Oorschot, “Graphical passwords: Learning from the first twelve years,” ACM Comput. Surveys, 2012.

[2]. The Science Behind Passfaces [Online]. http://www.realuser.com/published/Science BehindPassfaces.pdf

[3]. B. Hoanca and K. Mock. Password Entry Scheme Resistant to Eavesdropping, Security and Management, Las Vegas, Nevada, 2008.

[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]. D. Weinshall, “Cognitive authentication schemes safe against spyware,” in Proc. IEEE Symp, 2006.

[6]. P. Dunphy and J. Yan, “Do background images improve ‘Draw a Secret’ graphical passwords,” in Proc. ACM CCS, 2007.

[7]. D. Florencio and C. Herley. KLASSP: Entering Passwords on a Spyware Infected Machine. Using a Shared-Secret Proxy, 22nd Annual Computer Security Applications Conference (ACSAC), 2006, pp.67-76.

[8]. S. Chiasson and R. Biddle, “Graphical password authentication using cued click points,” in Proc. ESORICS, 2007, pp. 359–374.

[9]. 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. 2008.

[10]. 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.

[11]. L. Wang, H. Gao, X. Liu and U. Aickelin, “Against Spyware Using CAPTCHA In Graphical Password Scheme,” in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl., Jun. 2010, pp. 1–9.

[12]. Taekyoung Kwon, 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.

[13]. Haichang Gao, "A New Graphical Password Scheme Resistant to Shoulder-Surfing", 2010.