GRAPHICAL CRYPTOGRAPHIC VERIFICATION SYSTEM

Mr. S. Balika J Chelliah
Assistant Professor, Department of Computer Science and Engineering, SRM University, Chennai, Tamil Nadu, India.
Email- balika888@gmail.com

Ms. M. Shobana
Department of Computer Science and Engineering, SRM University, Chennai, Tamil Nadu, India.
Email - shobanasofia333@gmail.com

Mr. Mandli Srikar Reddy
Department of Computer Science and Engineering, SRM University, Chennai, Tamil Nadu, India.
Email - srikarr004@gmail.com

Abstract - A Graphical Cryptographic Verification System that restores the static digital pictures naturally used in graphical password systems with personalized physical tokens, here in the form of digital pictures showed on a physical user-owned device such as a mobile phone. Users present these pictures to a scheme camera and then enter their password as a sequence of selections on live video of the token. Extremely distinctive optical characteristics are extracted from these selections and utilized as the password. We present three probability studies of examining its consistency, usability, and safety against surveillance. The consistency study Graphical Cryptographic Verification System demonstrates that image-feature based passwords are viable and suggests appropriate system thresholds password items should include a minimum of seven features, 40% of which must geometrically equal unique stored on an authentication server in order to be moderator equivalent. The usability study calculates task completion times and error rates, revealing these to be 7.5 s and 9%, broadly comparable with preceding graphical password systems that use static digital images. In the end, the safety study highlights Graphical Cryptographic Verification System conflict to observation attack three attackers are able to compromise a password using shoulder surfing, camera based observation, or malware. These results indicate that Graphical Cryptographic Verification System shows promise for safety while maintaining the usability of current graphical password schemes.

Keywords— Graphical Cryptographic, Graphical password, input, live video, observation, user study.

1. Introduction

Secure access to information underpins recent digital schemes and services. We maintain our communications, financial data, work documents, and personal media safe by providing identity information and then authenticating to that identity. Text passwords and personal identification numbers (PINs) are the dominant authentication method [1] as they are simple and can be deployed on systems including public terminals, the web, and mobile devices. However, passwords suffer from limitations in terms of memorability and security passwords that are difficult to guess are also hard to remember. This is a major problem as an average user possesses 25 online accounts secured with up to six different passwords [2] and representing a substantial memory burden. To deal with this problem, individuals adopt non-secure coping strategies such as reuse of passwords across systems, noting down passwords, or simply forgetting them entirely [3]. In order to mitigate these problems, researchers have proposed graphical password schemes that rely on input such as selecting portions of an image. These systems have been shown to improve memorability without sacrificing input time or error rates [4] while also maintaining a high resistance to brute force and guessing attacks.

However, graphical passwords present their own problems. One issue is their susceptibility to intelligent guessing and shoulder-surfing attacks [5]. Such attacks are efficient since the parts of images that clients select as password pieces are both easy for an attacker to monitor by snooping over shoulders or setting up a camera to evidence input and also comparatively predictable users tend to choose hotspots such as the eyes in a facial portrait [6]. This problem is addressed mainly as the image substances for Graphical Cryptographic Verification System are typically stored on verification servers and readily presented to attackers in response to input of easily accessible user identity information [7].

To address this issue, we present a new point-click Graphical Cryptographic Verification System, Graphical Cryptographic Verification System Bring Your Own Picture that increases resistance to observation attack by coupling the user’s password to an image or object physically possessed [8]. This is accomplished by utilizing live image of a physical token, such as an object, a photograph, or even an image of a body part (e.g., a palm), as the canvas for entering a graphical password. This physical object restores simply available server-based images, and we dispute that attackers will struggle to capture useful replicas of this content. We present an implementation for the scheme based on SIFT image features [9] and a demonstration of its viability through three feasibility studies covering: 1) the reliability and robustness of Graphical Cryptographic Verification System feature based input; 2) participant task performance times and error rates using Graphical Cryptographic Verification System; and 3) the security of Graphical Cryptographic Verification System against observation attack.

2. Related Work

Graphical password systems are knowledge-based verification methods that influence peoples’ capability to memorize and recognize visual information more readily than alphanumeric information. Researchers have explored three broad types of graphical passwords: recall-based draw metric schemes based on sketching shapes on screen, recognition-based cognometric schemes based on selecting known items from large sets of options, and cued-recall loci-metric schemes based on selecting regions of pre-chosen images. Loci-metric schemes are discussed as is multifactor authentication [10], as it relates to Graphical Cryptographic Verification System and its combination of a token, or something you have, on which a password, or something you know, is entered.

A great many graphical password schemes have been proposed as alternatives to text-based password authentication. We provide a comprehensive overview of published research in the area, covering usability and security aspects, as well as system evaluation. The paper first catalogues existing approaches, importance new characteristics of selected methods and recognizing key usability or security advantages [11]. We then review usability requirements for knowledge-based authentication as they apply to graphical passwords, identify security threats that such systems must address and review known attacks, discuss methodological issues connected to experimental assessment, and recognize areas for additional investigate and improved methodology.

The term “CAPTCHA” was first introduced in 2000 by von Ahn et al., illustrating a test that can distinguish human beings from computers [12]. Under general explanations, the test must be: Easily solved by humans, easily generated and evaluated, but not easily solved by computer. Over the past decade, an amount of dissimilar methods for generating CAPTCHAs have been developed, every satisfying the properties described above to varying degrees. The main generally establish CAPTCHAs are visual challenges that need the user to recognize alphanumeric characters current in an image obfuscated by some combination of noise and distortion. The necessary challenge in designing these obfuscations is to build them simple sufficient that users are not dissuaded from attempting a solution, yet still too difficult to solve using available computer vision algorithms [13].

Defeating automation has received far more attention and has kicked off a competition of sorts between those building ever more sophisticated algorithms for breaking CAPTCHAs and those creating new, more obfuscated CAPTCHAs in response.

In pure recall based graphical password schemes, users need to reproduce their password without being given any hints or cues [14]. Alphanumeric passwords, as well as manuscript signatures, are instances of indicates of authentication based on pure recall. Jeremyn et al. Described a graphical password scheme “Draw a Secret” (DAS), where users draw a shape on a grid. Users need to illustrate approximately the similar shape in order to validate themselves. Study [15] a variation of DAS. Recent research describes possible dictionary attacks against DAS. Overall, graphical password schemes based on pure recall are rapid and convenient to utilize, however they seem to have the same disadvantage as alphanumeric password: They are hard to remember with sufficient precision when they have enough entropy to be secure.

3. Proposed System

Graphical Cryptographic Verification System seeks to make graphical passwords more secure against intelligent guessing and shoulder-surfing attacks. We argue these weaknesses stem from the ease with which both password contents and password canvases can be observed or, in the case of canvases, directly accessed from a server. Graphical Cryptographic Verification System tackles this problem by introducing a physical token into the authentication process. This way, Graphical Cryptographic Verification System transforms a graphical password, which is traditionally a single factor authentication mechanism, to a more secure multifactor authentication method. We dispute that this makes Graphical Cryptographic Verification System Resilient-to-Internal-Observation, meaning that an attacker cannot impersonate a user simply by intercepting input on the authentication device or by eavesdropping on the communication between the authentication device and verification system.

Assuming users have previously created a password, login involves users identifying themselves at a Graphical Cryptographic Verification System terminal in a manner fitting the system and use context. For example, systems such as office door locks may assume all users are valid, while a user ID might be used on a public computer, and higher security applications, such as a bank ATM, will likely rely on a physical token such as an ATM card. Graphical Cryptographic Verification System could be integrated into any of these scenarios. Second, users place a pre-chosen password image or object they possess on top of a camera unit in the terminal. This is captured and displayed live on an adjacent touch screen. Third, they tap on the picture locations that correspond to their password. This way, authentication requires both the physical token and the password simultaneously. We argue this raises the resistance of Graphical Cryptographic Verification System to attacks based on password observation and guessing as attackers need to possess a user's genuine token or a high fidelity copy.

We present a new point-click graphical password system, Graphical Cryptographic Verification System Bring Your Own Picture that increases resistance to observation attack by coupling the user's password to an image or object physically possessed. This is realized by utilizing live image of a physical token, such as an entity, a photograph, or even an image of a body part (e.g., a palm), as the canvas for entering a graphical password. This physical object replaces easily accessible server-based images, and we argue that attackers will struggle to capture useful replicas of this content. Users place a pre-chosen password image or object they possess on top of a camera unit in the terminal. This is captured and displayed live on an adjacent touch screen. They tap on the image locations that correspond to their password. This way, authentication requires both the physical token and the password simultaneously.

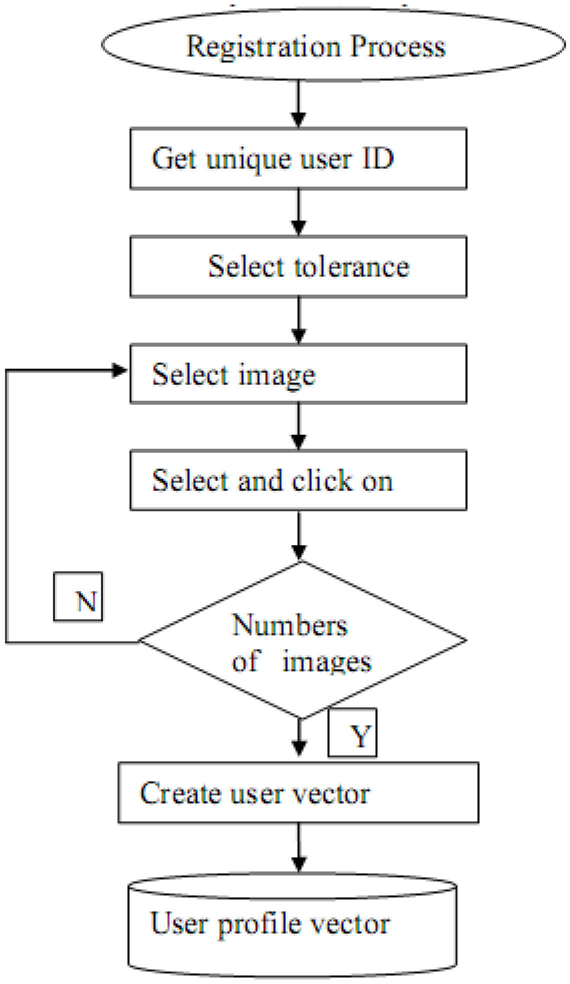

Fig.1. Flow Diagram

4. Implementation

4.1. Registration Module

Fig.1 shows this module is divided into 3 stages. First is Account Creation which is followed by Password Creation and finally Deciding sequence of images presented or selected. The user has to effectively generate his account first. In this system, each user is identified by a unique username. Therefore to create that every user has a unique username, the scheme previous to creating an account checks for the availability of username. If the Username specified by user already exists, then the system prompts for the availability of that name.

4.2 Picture Selection

In picture selection stage there are two methods for selecting picture password authentication. The user can select pictures of his choice or can directly get the images from database.

4.3 User-Defined Pictures

Images are selected by the customer from the hard disk or any other image supported devices.

4.4 System-Defined Pictures

Images are selected by the customer from the folder of the password system.

4.5 Login Phase:

logging to the picture based Authentication System, the user is presented with the first picture which he had utilized through registration time. While logging, the viewport will not be visible and the user has to click on his registered click-point on the image. Because it is almost impossible for a human being to click on the exact point, therefore a tolerance value is hard coded in the system. The tolerance value (D) indicates the degree of closeness to the actual click-point. Euclidean distance is calculated to find the distance between two click points. Euclidean distance between two points' p and q is given by-

$$d(p,q) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2 + \cdots s + (p_n - q_n)^2}$$

$$= \sqrt{\sum (p_i - q_i)^2} \;\; i = 1 \; to \; n$$

Above distance is computed for every picture and if this distance comes out less than a tolerance value D then only next registered image is exhibited. The value of D is taken as 5 in our system. Therefore, if the click-point falls inside the scheme described tolerance square then only the next right image will be displayed to the user, else a random picture will be displayed which may lead the user to the wrong path. The next picture displayed is forever based on the position of the before entered click-point, creating a path through an image set. Thus a wrong click leads to an incorrect path, with an explicit indication of authentication failure only after the final click. Only it is successful completion of this process.

5. Conclusion:

Conclusion of this paper projected improving the safety of Graphical Cryptographic Verification Systems by integrating live video of a physical token that a user carries with them. It first demonstrates the feasibility of the concept by building and testing a fully functional prototype. It then illustrates that user performance is equivalent to that attained in standard graphical password systems through a usability study assessing task time, error rate, and subjective workload. Finally, a security study shows that Graphical Cryptographic Verification System substantially increases resistance to shoulder-surfing attacks compared with existing graphical password schemes. Ultimately, we argue this paper demonstrates that Graphical Cryptographic Verification System conserves the beneficial properties of graphical passwords while increasing their security.

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] D. Davis, F. Monrose, and M. Reiter, “On user choice in graphical password schemes,” in Proc. USENIX Security, pp. 1–11, 2004.

[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., pp. 1–15, 1999.

[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 user-drawn 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, pp. 343–358, 2007.

[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, pp. 20–28, 2007.

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

[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.

[11] D. Weinshall, “Cognitive authentication schemes safe against spyware,” in Proc. IEEE Symp. Security Privacy, pp. 300–306, May 2006.

[12] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, “CAPTCHA: Using hard AI problems for security,” in Proc. Eurocrypt, pp. 294–311, 2003.

[13] 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., pp. 121–130, 2008.

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

[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.