ADVANCE GRAPHICAL PASSWORD SYSTEM FOR SECURITY USING YOUR OWN IMAGE

[1]AISHWARYA A. PRABHUSALGAONKAR, [2]NEHA A. KAROL, [3]VINDA G.NAGWEKAR

[1,2,3]Computer Engineering Department, SSPM'S COE, Kankavli
E-mail: [1]aishwarya.prabhu07@gmail.com, [2]nehanasim318@gmail.com

Abstract— Advance Graphical Password For Security Using Own Image is a new graphical password scheme that replaces static images used in graphical password system with our own images which are stored in devices such as mobile phone. User provide this image to system and enter the password as a sequence of selection of portions from the image. Features are extracted from selection and used as a password. This system is resistant to observation attack- shoulder surfing, camera based observation. Thus system provides security while maintaining the usability of current graphical password scheme.

Keywords— AGPS, Graphical Password, Security.

I. INTRODUCTION

Secure access to information underpins modern digital systems and services. We keep 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 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 and representing a substantial memory burden. To deal with this problem, individuals adopt no secure coping strategies such as reuse of passwords across systems, noting down passwords, or simply forgetting them entirely. 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 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. Such attacks are effective because the sections of images that users select as password items are both easy for an attacker to observe by snooping over shoulders or setting up a camera to record input and also relatively predictable users tend to choose hotspots such as the eyes in a facial portrait. This issue is particularly problematic as the image contents for graphical password systems are typically stored on authentication servers and readily presented to attackers in response to input of easily accessible user identity information.

To address this issue, we present a new point-click graphical password system, AGPS Using Your Own Image, that increases resistance to observation attack by coupling the user's password to an image physically possessed. This is achieved by providing 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. We present an implementation for the scheme based on SIFT image features and a demonstration of its viability through three feasibility studies covering:

1) The reliability and robustness of AGPS feature based input 2) Participant task performance times and error rates usingAGPS 3) The security of AGPS against observation attack.

II. RELATED WORK

Graphical password systems are knowledge-based authentication techniques that leverage peoples' ability 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 econometric schemes based on selecting known items from large sets of options, and cued-recall loci metric schemes based on selecting regions of prechosen images. Loci metric schemes are discussed as is multifactor authentication, as it relates to AGPS and its combination of a token, or something you have, on which a password, or something you know, is entered.

2.1. Loci metric Password Schemes

Cued-recall (loci metric) password schemes involve user's selecting regions on one or more images. Blunder's U.S. patent is the earliest example. A seminal example is Pass Points. During login, users are shown a previously selected image, and they enter a password by clicking on a sequence of locations on the image. Authentication is successful if the XY

coordinates of these clicks match a previously stored set of password points. A longitudinal study resulted in login times of 8.78 to 24.25 s and a failed authentication rate of 7–13%.

While simple and effective, cued-recall graphical passwords present new security issues. For instance, users typically select hotspots, locations on an image that are highly distinguishable, memorable, and also predictable to attackers. In the Microsoft Windows 8 graphical password system, the most common password involved a photo of a person and triple tapping on the face, where one of the selection points was an eye. Addressing this issue, the cued-click points (CCP) system presented a series of images and allowed users to select only a single point per image, reducing the need to select com- mon hotspots. Evaluations of this technique led to authentication times in the range of 7–8 s and success rates of 90–96%.A second key problem with loci metric systems is observation, as password click-points can be acquired by attackers after viewing a single authentication process. Securing against observation attack for graphical password systems is critical. Caisson et al. Remark: "User interface manipulations such as reducing the text size of the mouse cursor or dimming the image may offer some protection, but have not been tested." One exception is a variant of CCP that uses eye-tracking technology for input. This system increased resistance to observation but negatively impacted performance: login times rose to 47.1–64.3 s and only 67% of participants successful authenticated on their first attempt. Although more secure, this technique was prohibitively slow and error prone.

2.2. Multifactor Authentication Schemes

Multifactor authentication is based on the combination of two or more independent processes, can boost security. In typical multifactor authentication schemes, physical tokens are used to generate and store secrets for user authentication. While these tools offer increased security, they are susceptible to particular kinds of attack, such as Man-in-the-Middle schemes that snoop on, or alter, messages transmitted between a user and the system.

AGPS is a multifactor authentication system both a physical token and a password are needed to authenticate. AGPS differs from prior approaches in three ways. First, it is more flexible instead of posing restrictions on the form of tokens, any sufficiently complex image or object can be used as a AGPS token. Second, the two authentication factors are tightly coupled the password factor is entered on the token factor. We suggest this close relationship will make the scheme easy to understand. Finally, the image tokens in AGPS are high-entropy, sufficiently so that they have been previously pro-posed as a single factor authentication scheme. We also suggest that these physical data-rich tokens will be resistant to Man-in-the-Middle schemes as attackers will face substantial barriers in terms of capturing tokens in sufficient detail to support successful hacks.

III. OVERVIEW

AGPS 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. AGPS tackles this problem by introducing a physical token into the authentication process. This way, AGPS transforms a graphical password, which is traditionally a single- factor authentication mechanism, to a more secure multifactor authentication method. We argue that this makes AGPS 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.

AGPS authentication takes place as follows. Assuming users have previously created a password, login involves users identifying themselves to the system and use context. Second, user connects its mobile phone to the system and allow it to transfer files. Third, they open the image from the camera on the system and select the image 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 AGPS to attacks based on password observation and guessing as attackers need to possess a user's genuine token or a high fidelity copy.

Fig. Overview of the system

IV. PROPOSED WORK

There is one computer running the AGPS system. First user should provide authentication to that system. The system is useful for different applications present on the computer or for web applications. They should connect their mobile phone to the computer. Then by unlocking the phone they have to choose the option of allowing file transfer. By allowing this user can see the data from the mobile phone on the computer. Then they can go to the

particular image file location and can open the image. By selecting the portions of the image using the in a particular sequence they can create their password. Here the order of selection is also important.

In existing graphical password systems, the passwords are represented as the XY image coordinates of selections. This technique does not work with AGPS. Instead, AGPS selections are stored on the authentication server as a set of optical features computed with the SIFT image processing algorithm. This was achieved by capturing a 140 × 140 image subsection around the centre point of each password item A Gaussian blur was then applied and Lowe's SIFT algorithm was computed with the peak threshold set to 2 and the edge threshold set to 10. This yields a list of image features and descriptors. Those that fell outside the central 70 × 70 selection box were discarded and the remainder used for password matching [see Fig. 3(d)]. The matching process involved minimizing the Euclidean distance between the sets of feature points in the original and entered password items. Subsequently, a threshold on the percentage of matching features was used to determine whether the entered password matched the original. Lower threshold levels result in a lenient password system, whereas higher levels are stricter. This process hinges on the fact that SIFT features are highly distinctive, robust to noise, accurate, and rotation invariant—capable of matching the features extracted from a single image against a database containing 100000 images with an overall accuracy of 80%.

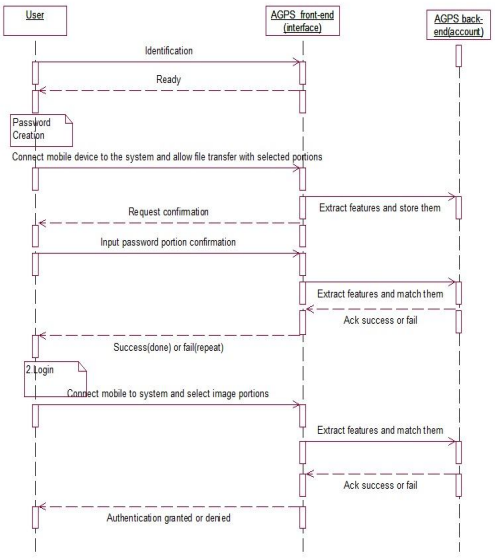

Fig.- Sequence diagram of the system

V. SECURITY ANALYSIS

This section provides a security analysis of the AGPS system. We can analyze the system for following issues:

5.1. Theft

While AGPS cannot be prevent theft, its close coupling of a token to a password does provide benefits. Unlike many types of authentication tokens physical possession is insufficient to crack the system. Attackers must also gain access to the password. This way, AGPS offers advantages over purely token-based systems, including those based on secure device pairing over visual channels. There are also three further advantages conferred by using a token displayed on a mobile device. First, attackers must unlock the mobile device to access the token, potentially facing an additional and unrelated security scheme. Second, they must identify the precise token image, a potentially challenging process. Third, users could conceivably use software to remotely wipe a token from a stolen device. Thus AGPS password images provides a measure of resistance to attacks based on token theft over and above that present in more traditional token-based schemes.

5.2. Educated Guessing or Brute Force Attacks:

From a security perspective, typical cued-recall graphical passwords have practical password spaces comparable in cardinality to four- or five-digit PINs. Data from the feasibility study suggest that AGPS has a similarly sized password space with a matching threshold of 40%, the heatmap analysis indicates that each AGPS selection has a viable radius of 35 pixels (0.75 cm), leading to a valid selection area of 0.56 cm^2 , a figure very close to that used in benchmark systems such as the 0.53cm^2 used in PassPoints. Thus, given a total selection space of 450 × 500 pixels, the total number of discriminable selection points for each user input is approximately ~220. Over a four-item PIN, according to the calculations used by Wiedenbeck *et al.* this leads to a total Hartley entropy (or available password space) of ~ $\log_2$ (220.4^4), a figure greatly exceeding that of a four-digit numerical PIN.

We acknowledge that these entropy figures are optimistically high and represent a theoretical maximum in reality, only a subset of the possible hotspots are actually likely to be selected However, this entropy calculation appears in closely related work, and using this common formulation makes AGPS comparable with prior work. We also note that in contrast with other graphical password schemes, AGPS use of a token makes guessing attacks insufficient if used alone they must be combined with theft or observation in order to also acquire either the users token or a high fidelity copy. We argue that this increases the security of AGPS relative to prior approaches.

5.3 Observation:

Cued-recall graphical passwords are vulnerable to observation attacks. A single observation can be enough to disclose a password to a bystander.

Reflecting the importance of this vector, an observation attack was staged on the AGPS system to empirically assess the system's resistance to this type of threat. Three types of observation were considered: shoulder-surfing, a camera attack, and an atttack based on malware that takes over the AGPS terminal and records the image displayed on the screen and the coordinates of the input points selected by the user. This last attack represents a worst case scenario a substantial and comprehensive man-in-the-middle attack akin to using the system camera to skim not only the password items entered, but also a copy of the image they are entered on.

CONCLUSION

An important usability and security goal in authentication systems is to help user to select better passwords and thus increase the effective password space. We believe that users can be persuaded to select stronger passwords through better user interface design. AGPS encourages and guides users in selecting more random graphical passwords. A key feature in AGPS is that creating a secure password is the "path-of-least-resistance", making it likely to be more effective than schemes where behaving securely adds an extra burden on users. The approach can prove effectiveness at reducing the formation of hotspots, avoid shoulder surfing problem and also provide high security success rate, while still maintaining usability.

REFERENCES

[1] G. E. Blonder, "Graphical passwords," U.S. Patent 5 559 961, 1996.

[2] S. Chiasson, P. C. van Oorschot, and R. Biddle "Graphical password authentication using cued click points," in Proc. 12th Eur. Symp. Res. Comput Security, 2007, pp. 359–374.

[3] S. Chiasson, A. Forget, R. Biddle, and P. C. Oorschot, "User interface design affects security: Patterns in click-based graphical passwords, Int. J. Inf. Security, vol. 8, no. 6, pp. 387–398, 2009.

[4] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. C. Van Oorschot, "Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism," IEEE

[5] Trans. Dependable Secure Comput., vol. 9, no. 2, pp. 222–235, Mar./Apr. 2012.

[6] N. Saxena, J. E. Ekberg, K. Kostiainen, and N. Asokan, "Secure device pairing based on a visual channel

[7] (short paper)," in Proc. IEEE Symp. Security Privacy, 2006, pp. 306–313.

[8] F. Tari, A. Ozok, and S. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," in Proc. 2nd Symp. Usable Privacy Security, 2006, pp. 56–66.

★★★