GRAPHICAL AUTHENTICATION FOR SECURE SOCIAL NETWORKS

Lebogang Mametja
University of Cape Town
mmtleb002@myuct.ac.za

ABSTRACT

Graphical password schemes have been proposed as an alternative authentication method to text-based systems. This proposal is based on the premise that humans are better at recognising visual images than text-based data. The paper will provide an overview of graphical password schemes in the context of social networks. These schemes are classified into two categories: recall-based and recognition-based approaches, with DAS and Passfaces being the primary exemplars in each category. The paper will then compare and evaluate these approaches with text-based ones in terms of usability and security.

Keywords: Graphical passwords, recall, recognition

INTRODUCTION

The constraints and goals of authentication systems differ depending on the intended environment of use. It is acceptable for high-risk domains to have slightly more complex systems which are more difficult to use, in order to achieve high-levels of security. On the other hand, low-risk domains, such as social networks, should provide quick and easy logins which are relatively less secure [2].

This is echoed by Hong [8] who states that security should only be increased if it will be effective in practice. The paper discussed a study which analysed 75 password policies and found results which were counterintuitive: the most attacked, valued and largest companies allowed relatively weak passwords because they wanted their systems to be usable. This was contrasted by the stricter policies unnecessarily incorporated by government and schooling institutions [15].

Due to their visual nature, graphical password schemes are more prone to shoulder-surfing attacks [Tari]. It is desirable for social networks to be shoulder-surfing resistant because they are frequently accessed in environments which are conducive to such attacks (for example, public areas) [17]. As such, this paper will provide a comprehensive overview of shoulder-surfing resistant approaches.

Adding more security, however, has a trade-off of less functionality [6, 14] - and it is this trade-off that will be the prime focus of this paper. Moreover, this trade-off will be analysed in the context of social networks. The schemes discussed will be based on the principles of recall and recognition, with DAS and Passfaces chosen as the exemplars in each category. This is due to the extensive study that has been conducted on each of them. The paper will conclude by highlighting possible areas for further research.

RECALL

Draw-a-Secret (DAS) [9] is the most studied recall-based graphical password scheme for various reasons. First, its theoretical password space is higher than text-based ones; and second, DAS can be used not only for user authentication, but also for key generation [4]. The authentication process consists of an N x N grid on which the user draws their password using a stylus on PDAs or a mouse on the computer. A drawing consists of a single or several pen strokes separated by pen ups. The system encodes the drawing as a series of coordinates of the grid cells passed through in the drawing.

Although stylus pens may aid the user in avoiding fuzzy boundaries (which are illegal crossings made by tracing grid lines or crossing through cell corners) [4, 9], they are less frequently used today. An enhanced drawing encoding algorithm is needed to allow users to interact directly with the system through touch screens on mobile phones.

Moreover, Dunphy and Yan [4] found that participants with non-technical backgrounds had more difficulty understanding the system. Thus, removing these grid crossing restrictions altogether would increase the usability of the system. The paper further suggested a period of enrolment to help users practice and commit passwords to memory, and a step-by-step undoing to further help them with this process.

Also in [4], success rates that ranged from 57-80% were found through the testing of DAS with paper prototypes. The paper expressed concern over the credibility of the results due to the prototype medium, and further commented that more research would be needed to explore the possibility that the effective password space could be smaller than the theoretical one.

Coping strategies used in text-based password schemes include writing down passwords and re-using passwords across accounts [15, 16]. William [15] did not consider the former a serious threat anymore because network hackings had become the common form of attacks. He considered the latter more serious as it translated into a single point of failure. Yan et al. [16] proposed a more sophisticated strategy called Pass-phrase, which involved using the first letter of a phrase to generate a password; for example, a phrase like “My uncle and aunt have 12 cousins” would generate the following password: “Mu&ah12c”. The effectiveness of this strategy has not yet been analysed.

In DAS, users chose symmetry and centring the image to help with memorability [13]. These strategies decreased the effective password space although it is not clear by how much, due to lack of implementation and suitable user studies [2]. A separate study [9, 13] further revealed that the effective password space was decreased by few stroke counts, and proposed a Grid Selection technique to increase this password space.

This technique involves a grid that is initially large. The user selects a drawing grid which will be zoomed in, allowing the user to enter their password. In theory, this could add 16 bits to the password space; however, no user study has been carried out to test how it would work in practice [4, 9].

Three shoulder-surfing resistant approaches were studied by Zakaria et al. [17], namely Decoy Strokes, Disappearing Strokes and Line Snaking. In the Decoy Strokes defence, decoy stokes were drawn at the same rate as the user’s and in a slightly different colour. This was done to distract the onlooker from the user’s real password. Disappearing Strokes involved removing the user’s stroke from the screen after being drawn. It was found to be optimal for multiple strokes.

In the last approach, the start of the user's password would disappear as the user was still drawing the password, thereby preventing the attacker from seeing the complete user stroke on screen. This approach was optimal for long singular strokes.

The paper conducted a 68-user and a separate 34-user study to compare the three defence techniques. They found that 63% of DAS passwords were completely stolen with the Decoy Strokes approach, 14% from the Disappearing Strokes defence and none from the Line Snaking defence. The results supported their hypothesis that the Line Snaking defence would work better than Disappearing Strokes, and that Decoy Strokes would be the weakest of all defences.

The paper then conducted a 30-user study comparing the usability of the defence techniques. The Line Snaking defence had the highest average login time at 8.3 seconds and needed more attempts to login with a 1.3 second error rate. It was also found that the Disappearing Strokes defence was preferred more than the Line Snaking one. Its average login time and error rate were 7.1 seconds and 1.1 seconds, respectfully. All these results supported their corresponding hypotheses.

Of the 65% participants who preferred the Disappearing technique, 67% immediately saw the security advantage of Line Snaking but preferred something they were comfortable with using. This showed that usability is more important to users than security.

One limitation to the study is that there was only real-time viewing of the passwords - no camera or video recording equipment was used. Another limitation is that participants did not use their own passwords thereby affecting memorability.

More generally

Background Draw-a-Secret (BDAS) [4] sought to improve password strength by adding background images with the aim of encouraging users to enter more complex, and less predictable passwords. Results showed that this goal was achieved as the average strength improved by 10 bits. Another result was that of improved memorability: users had the option of using these background images in one of three ways: either to use the image to map various features of their drawing, to use the system as cued-recall, or both. Dunphy and Yan [4] further commented that a proactive password checker would be more useful in this context because users where more encouraged.

One limitation to the study was the lack of a test on long-term memory recall. Another limitation was that it was implemented via a paper prototype and therefore issues such as interference and robustness to shoulder-surfing attacks could not be explored.

Other shoulder-surfing resistant methods use finger pressure [10] and special hardware such as screen filters [1]. The finger pressure technique was resistant to more dedicated shoulder-surfing methods such as video recording the password being entered, but was found to be unusable because users applied little to no pressure when drawing. Furthermore, the study found that people were reluctant to change and would not easily switch to a new scheme: only 64% of testers were willing to change from text-based passwords to a more secure graphical password scheme.

The Amzer® screen filters use a polarization technique to enhance the privacy of its users. It enables users to see from the front, but is dark when viewed from the side at an angle of more

than 30 degrees. Although effective, it requires additional costs. Text-based passwords are ubiquitous because other methods are costly or require special hardware [14].

Generally, in [13], recall-based systems are less vulnerable to brute-force, malware and social engineering attacks than text-based passwords. This is because of the complexity of automatically generating mouse motion to imitate human input, in brute-force and dictionary attacks. Mouse motion and keystroke loggers would not be effective on their own, but would be effective when coupled with screen scrapper malware [2]. In terms of social engineering, screen shots, sketches or notes could be used to aid attackers [5].

Password reset and change policies were found to be costly in text-based systems: Tari et al. [14] found that 30% of helpdesk calls were for password resets alone. This can be translated as a loss in worker productivity. Hong [8] suggested the review of budget costs of implementing needlessly high-secure policies.

In contrast, graphical passwords cannot be reset as easily as text passwords because they are hard to describe [18]. One solution is to assign a temporary non-graphical password during password reset, giving system access to create a new password [2]. Nevertheless, the low-risk domain of social networks does not require such stringent security measures.

RECOGNITION

The Passfaces authentication procedure involves users preselecting a set of human faces. During login, a panel of candidate faces will be presented to the user, who must select the face belonging to their set from among decoys. Several such rounds are repeated with different panels. For successful login, each round must be executed correctly [2].

The main advantage of Passfaces is that the task of recognizing visual data is easier than having to recall something from memory [2]. The rationale behind this technique is that human faces can be recalled more easily than other image types [18]. However, Dunphy and Olivier [3] revealed that the optimal image types were icons and photos used the in Komanduri and Tullis & Tedesco authentication procedures, respectfully. Both procedures had 100% success rates while the success rate for Passfaces was only 85%.

Zangooei at al. [18] compared Passfaces with text-based schemes and found that Passfaces had a third of the login failure rate than text-based passwords. Suo et al. [13] found Passfaces passwords to be memorable over long intervals. Everitt et al. [5] found Passfaces to be a suitable alternative to text-based passwords where text-input was difficult or limited (for example, mobile phones). It was further found that it was resistant to social engineering attacks because the things that stand out (and are thus descriptive) are cropped, leaving just a single face which is hard to describe.

The main disadvantage was that the Passfaces login time was slow and took longer than that of text-based authentication systems [13, 18]. This is because the user would be required to scan many images to identify a few pass-images. The password initialization process also took long because it required the user to pick pass-images from a large set of selections [13].

Zangooei et al. [18] further found that Passfaces required extra storage for storing images corresponding to each user and required extra maintenance of that database. Network transfer delays were of special concern as the system needed to display a large number of images for each round of the login process.

Tari et al. [14] did a study to compare the perceived and real shoulder-surfing risk between text-based and graphical passwords. The paper explored the possibility of whether Passfaces would be able to fulfil both the security and usability requirements. It conducted a 20-user study to compare four configurations: mouse and keyboard entry for Passfaces, and strong and weak text-based passwords.

Participants both perceived and experienced a higher level of vulnerability of Passfaces with mouse to shoulder-surfing. Of the four configurations, Passfaces keyboard entry was the least vulnerable to shoulder-surfing. This was possibly due to the speed entry with the keyboard and the need for the attacker to look in two places at once. Curiously, the participants did not perceive the Passfaces with keyboard to be less vulnerable and there was no statistically significant correlation between real and perceived vulnerability for this configuration.

A surprising result was that strong text-based passwords proved to be the most vulnerable to shoulder-surfing attacks. This seemingly counterintuitive result showed that high security against dictionary attacks did not translate to high security against shoulder-surfing attacks. The strong text-based password systems were vulnerable because attackers aimed to capture each character one by one, not focusing on the meaning of the password.

Users with weaker text passwords tended to enter their passwords faster than strong, text-based password holders. This was an example of how the usability of a system could actually increase its security. Speed of entry made it difficult for an attacker to capture weak text-based passwords. The study removed the myth that strong text passwords are universally better than weak passwords; that is, it showed the importance of context. In the context of social networks, emphasis should be placed on usability.

There were several limitations to this study: firstly, there was only real-time viewing of the passwords - no camera or video recording equipment was used. Secondly, the study did not include a test on long-term memory recall and lastly, the entry speed was constant but not controlled.

More generally

Sobrado and Birget [12] discussed three other shoulder-surfing resistant approaches: firstly, a Triangle scheme , where the user is required to click inside the convex hull formed by 3 pass-objects (out of K previously chosen pass-objects amongst decoy images). It uses a large number of pass-icons to confuse shoulder surfers trying to determine the correct pass-icon. The disadvantage of this system was that more effort would be required from the user, who would need to scan all these icons in order to find their pass-icons.

Secondly, a Movable Frame scheme where the user must now locate 3 out of K pass-objects. This time however, only 3 pass-objects are displayed at any given time and only one of them is placed in a movable frame. The task of the user is to move the frame (and the objects within it, like a tape) by dragging the mouse around the frame until the pass object on the frame lines up with the other two pass-objects.

The last scheme uses the intersection of the invisible lines formed by 4 pass-objects (out of K previously chosen pass-objects). The user must click near the intersection of the two of these invisible lines, inside the convex quadrilateral formed by those 4 pass-objects.

Hayashi and Christin [7] discussed another approach called Use Your Illusion. It offered resistance to shoulder-surfing and social engineering attacks while allowing user-chosen passwords. This was achieved through distorting the images chosen by users to increase protection. However, this increased security was made at the expense of login time is 18 seconds on average.

Dunphy and Olivier [3] did a 2-part study on using an automated method for selecting images presented in a login challenge. The results followed the intuition that errors increased as decoy images were made to be more similar to key images, and found that login success rates were significantly affected by 40%. Login times were affected by 21 seconds and had median duration of 35 seconds. However, in terms of security, this automated method made it susceptible to interference, shoulder-surfing and social engineering attacks.

The study had several limitations: firstly, it did not study long-term memory recall; secondly, users were not able to use their own images; thirdly, participants had only a single attempt to recognize their images and lastly, images were only processed at pixel-level. The paper suggested more sophisticated methods of image processing as a future area of study.

Lastly, Everitt [5] conducted a 100-user 5 week study which also tested long memory recall after 4 months. The study measured difficulty, memorability and usability in terms of failure rate, attempts required for successful login and login times respectfully. In terms of frequency, it was found that participants who accessed passwords more frequently were able to authenticate in less time and with fewer attempts.

In terms of interference, it was found that participants who accessed four different password schemes a week where 10 times more likely to fail than ones who accessed only one. This showed that studies on usability of graphical passwords may be overestimated if not studied in correct context of multiple passwords.

Moreover, it was found that patterns of access while training multiple passwords significantly impacted later ease of access. Participants who trained on multiple passwords were more likely to fail than those who trained on a single one. Long-term memory recall was more successful for the latter group. In terms of coping strategies, 29% of the participants said they would attempt to use various methods of documenting their passwords, such as screen shots, sketches or notes.

One limitation to the study was that there was no overlap of faces appearing in the multiple passwords assigned to participants - therefore these results may have underestimated interference among multiple services that draws from the same user database.

CONCLUSION

Text-based passwords are ubiquitous due to ease of use, less costs, no need for special hardware and all users understand how the authentication process works [14, 15]. Moglen [11] states that replacement software should be responsible and should provide existing functions to users in a way that does not compromise their privacy or security. This means that graphical passwords should provide all of what text-based passwords currently offer in order to make the transition as smooth as possible.

From the literature reviewed, it is clear that graphical passwords still have a long way to go. However, Zangooei [18] argues that the trade-off within the text-based paradigm (simple and short passwords are easy to remember, but easily guessed and cracked; while random and long

passwords provide more security, but are harder to remember and use) is enough consider graphical passwords as a good alternative.

Possible areas of research for recall-based systems are numerous. They include evaluating the practical usability issues and security threats of DAS and DAS with Grid Selection through software implementations of these systems coupled with a suitable user study. Other areas include step-by-step undo operation to help users with practicing and committing passwords to memory and an enhanced drawing encoding system to remove reliance on outdated hardware like stylus pens for user input.

The main complaint in all recognition-based schemes is that the long process takes too long- possible areas of research would include studying graphical password schemes that would cater to the needs of users of a social network: ones which placed more emphasis on usability (in terms of reasonably low login times) while providing adequate security.

REFERENCES

[1] Amzer®. Amzer® Privacy Protector Shield For Blackberry curve 8530,BlackBerry Curve 3G 9300. Available at: http://www.amzer.com/Amzer-Privacy-Protector-Shield-P84116.html (Accessed 22 April 2013)

[2] Biddle, R., Chiasson, S., and van Oorschot, P. C. 2012. Graphical Passwords: Learning from the First Twelve Years. *ACM Computing Surveys (CSUR)*, vol. 44, 4, Article 19 (August 2012), 41 pages

[3] Dunphy, P. and Olivier, P. 2012. On Automated Image Choice for Secure and Usable Graphical Passwords. In *Proceedings of the 28th Annual Computer Security Applications Conference*, ACM Press, New York, pp. 99-108

[4] Dunphy, P. and Yan, J. 2007. Do Background Images Improve “Draw a Secret” Graphical Passwords? In *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS)*, ACM Press, New York, pp. 36-47

[5] Everitt, K., Bragin, T., Fogarty, J., and Kohno, T. 2009. A Comprehensive Study of Frequency, Interference, and Training of Multiple Graphical Passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM Press, New York, pp. 889-898

[6] Grossman, J., Livshits, B., Bace, R., and Neville-Neil, G. 2013. Browser Security: Appearances Can Be Deceiving. *Communications of the ACM,* vol. 56, 1, (January 2013), ACM Press, New York, pp. 60-67.

[7] Hayashi, E., and Christin, N. 2008. Use Your Illusion: Secure Authentication Usable Anywhere. In *Proceedings of the 4th Symposium on Usable Privacy and Security*, (Pittsburgh, PA, USA, July 23-25), ACM Press, New York, pp. 35-45

[8] Hong, J. 2013. Passwords Getting Painful, Computing Still Blissful. *Communications of the ACM,* vol. 53, 3, (March 2013), ACM Press, New York, pp. 10-11

[9] Jermyn, I., Mayer, A., Monrose, F., Reiter, M., and Rubin, A. 1999. The Design and Analysis of Graphical Passwords. In *Proceedings of the 8th USENIX Security Symposium,* vol. 8, ACM Press, New York, pp.1-1

[10] Malek, B., Orozco, M., and El Saddik, A. 2006. Novel Shoulder Surfing Resistant Haptic-based Graphical Password. In *Proceedings of the EuroHaptics Conference* (Paris, France, July 3-6)

[11] Moglen, E. 2013. Privacy and security the tangled web we have woven. *Communications of the ACM,* vol. 56, 2 (February 2013), ACM Press, New York, pp. 20-22.

[12] Sobrado, L. and Birget, J. C. 2002. Graphical Passwords.*The Rutgers Scholar*, vol. 4. Available at: http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm (Accessed 22 April 2013)

[13] Suo, X., Zhu, Y., and Owen, G. 2005. Graphical Passwords: A Survey. In *Proceedings of the Annual Computer Security Applications Conference* (Tucson, Arizona, December 5-9), IEEE

[14] Tari, F., Ozok, A., and Holden, S. 2006. A Comparison of Perceived and Real Shoulder-Surfing Risks Between Alphanumeric and Graphical Passwords. In *Proceedings of the 2nd ACM Symposium on Usable Privacy and Security (SOUPS)*

[15] William, C. 2013. Rethinking Passwords. *Communications of the ACM*, vol. 56, 2 (February 2013), pp. 40-44.

[16] Yan, J., Blackwell, A., Anderson, R., and Grant, A. 2004. Password Memorability and Security: Empirical Results, *IEEE Privacy & Security*, vol. 2 (5), pp. 25-31.

[17] Zakaria, N. H., Griffiths, D., Brostoff, S. and Jeff, Y. 2011. Shoulder Surfing Defence for Recall-based Graphical Passwords. In *Symposium On Usable Privacy and Security (SOUPS),* Article No. 6, ACM Press, New York

[18] Zangooei, T., Mansoori, M., and Welch, I. 2012. A Hybrid Recognition and Recall Based Approach in Graphical Passwords. In *Proceedings of the 24th Australian Computer-Human Interaction Conference,* ACM Press, New York, pp. 665-673