CS4203 Assessment 1
An Analysis of Graphical Passwords

Student ID: 080010830

March 6, 2012

1 Introduction

Graphical passwords have been suggested due to the simple fact that humans can remember images better than text [1, 2, 3, 4, 5, 6]. Paivio's "dual-coding theory" [7] is the most widely accepted and it suggests that images are assigned perceived meaning whereas text is represented symbolically [8]. This allows for passwords that are easier to recall, stronger and less vulnerable to attacks than text based passwords [9].

Graphical passwords are commonly assorted in three groups depending on how they are memorized and inserted: *recognition*, *recall* and *cued-recall* [10]. Thus, the three graphical password techniques that we will discuss, compare and contrast in this report are PassFaces$^{\text{TM}}$ [11] which is a recognition-based system, GrIDsure$^{\text{TM}}$ [12]; a recall-based system and PassPoints [13]; a cued-recall system.

PassFaces$^{\text{TM}}$ [11] is the most comprehensively studied recognition-based system [14]. The user pre-selects a group of human faces, then during login these faces will be presented and the user must select the ones picked up before among other random faces. It uses a system-assigned portfolio of faces that users will have to memorize during the training process.

GrIDsure$^{\text{TM}}$ [12] uses a 5×5 grid of digits where users are required to select and memorize a pattern that should consist of an ordered subset of these 25 grid squares.

PassPoints consists of a "arbitrarily chosen sequence of points" [13] in an image that the user has to memorize.

2 Current Trends or Research

In terms of current trends there seems to be a tendency to comprehensively study graphical passwords before disregarding text-based passwords. Nonetheless, research is very limited in the area, there are not many papers published and the existing ones were conducted with a small number of participants. Furthermore, graphical passwords do not inherently solve the problems of text-based passwords, and more research is needed in order to fully understand if they will be the norm in the future. However, it is foreseeable that there will be more consistent research in this area and possibly most of the common problems encountered during the writing of this report will be solved.

3 Memory Recall

Adams et al. [15] proved that short and easy to recall text-based passwords are preferred by users. However, graphical passwords can not be analysed in the same way as text-based passwords, and after Tulving et al. [16] concluded that recognition is a less difficult memory task than recall it was clear that recognition-based systems were easier for humans than recall-based system. There are nonetheless other concerns when evaluating memory recall, above all memory interference which is defined in cognitive psychology as "the impaired ability to remember an item when it is similar to other items stored in memory [17]; and password reuse which reduces the effort to create and remember a password, but it has great security risks due to the fact that once the attacker gains acess to the password they might also gain access to considerably valuable accounts, as described in more detail in section 5. Furthermore, Weinshall [18] stated that"time-consuming training" is required to help users memorize randomly selected passwords.

3.1 PassFaces^{TM} Memory Recall

PassFaces^{TM} [11] which is a recognition-based system has very satisfactory rates of success, as proved by Valentine [19] who conducted a study with 77 users and concluded that they had a "login success rates between 72% and 100% by the third attempt" for periods of time that were up to 5 months. Moreover, PassFaces^{TM} is capable of increasing security by adding extra rounds of faces but at cost of extra memory effort by the user [14]. Also, Everitt et al. [20] studied Passfaces^{TM} with randomly selected passwords and found that if users logged in multiple accounts using four different graphical passwords were ten times more likely to fail authentication than users whom logged in using a single graphical password.

Thus, it is still unproven how many extra rounds of faces is appropriate, so we have passwords that are very secure and not very difficult to memorize.

3.2 GrIDsure$^{\mathrm{TM}}$ Memory Recall

GrIDsure$^{\mathrm{TM}}$ [12] is a recall-based system which according to Brostoff et al. [21] has had good results in terms of usability. The main proof is the expressive log in success rate of 87% on first attempt with passwords of length four. However users choose predictable patterns so it is easier for them to memorize the password [22, 23, 21]. Furthermore, symmetric [23] and natural[1] [21] patterns were observed which reduce significantly the actual pattern space.

Craik and McDowd [24] concluded that recall tasks have worse performance than recognition tasks; thus users frequently use the interface as a cue, creating a cued-recall system out of a recall system.

3.3 PassPoints Memory Recall

Wiedenbeck et al. [13] stated that learning PassPoints was “much harder” than text-based passwords, mostly due to the fact that graphical passwords were a new concept to participants. Furthermore, they found that the most common difficulty was that participants frequently clicked outside the tolerance area, however for security reasons they argued that it would not be feasible to enlarge it. Nonetheless, after the initial learning phase 40% of the participants were able to enter their password ten times without errors, and 70% within three attempts.

In contrast, the least successful 20% had to make 17 to 20 invalid attempts in order to successfully log in. Thus, more research is required in order to make assertive conclusions.

3.4 Overall Memory Recall

PassFaces$^{\mathrm{TM}}$ [11] due to its recognition-based interface is an easier graphical password system to recall than grIDsure$^{\mathrm{TM}}$ [12] and PassPoints [13]. Valentine [19] achieved success rates between 72% and 100% by the third attempt

[1] Such as left-to-right and top-to-bottom.

compared with GrIDsure (87% on first attempt[2]) and PassPoints (70%). Also, it is clear that log in frequency and how passwords are chosen has a great impact on password memorability. Nonetheless, literature is not very conclusive regarding the retention of graphical passwords, specially when users have multiple passwords, where evidence [25] suggests that considerable recollection problems can be caused by interference. Wiedenbeck et al. [13] posit that if different images are used for each password it should produce less interference, however they are concerned that this approach would make it harder for users to remember which image belongs to which system. Further studies are needed in order to better understand this challenge. On a last note, all the techniques described lack memory aids for valid users, that would help them reduce their memory recalling effort.

4 Strength

In principle, a strong password offers a greater degree of security than a week password but it will usually be more complex and harder to memorize [26]. Thus, the ideal password should be easy to remember as well as very hard to crack [13], and that is precisely the problem researchers are trying to solve using graphical passwords.

4.1 PassFaces$^{\mathrm{TM}}$ Strength

PassFaces$^{\mathrm{TM}}$ is a system that can be very strong at the expense of users' effort in memorizing it. Nevertheless, it is still not clear how secure the system is, mostly because people tend to choose faces that are similar to themselves in a rather predictable manner.

4.2 GrIDsure$^{\mathrm{TM}}$ Strength

GrIDsure offers more security than traditional PINs. For example, Microsoft applied GrIDsure as part of two-factor authentication for IAG and UAG [27]. The lack of studies in the area make it hard to determine how strong GrIDsure is, especially due to the lack of techniques to compare it with.

[2] Passwords of length four are equivalent to a four-digit PIN, however, recall and cued-recall systems are more equivalent to text passwords of 8-characters-or-more.

4.3 PassPoints Strength

PassPoints is a fairly strong system, considering the fact that with just six click points – including .25 cm of tolerance area – it is possible to generate a greater number of passwords than 8-character Unix-style alphanumeric passwords [13]. Furthermore, PassPoints is based on images that include hundreds of possible click points which makes it possible to create large password spaces, it has a "robust discretization" which allows for "cryptographically hash PassPoints" making it secure for storage, and surprinsingly users did not seem attracted to the same click points even when there are salient areas in the image [13]. Thus, it creates the impression of being a reasonably robust system, however the study conducted by Wiedenbeck et al. [13] had a small sample of participants and further research is needed.

4.4 Overall Strength

As we have seen, all the techniques analysed are acceptably strong and perhaps possible of being implemented in real life. However it is still unproven if the choices of a user would reduce the password strength. Moreover, graphical passwords seem to be easier to predict and that causes a great security risk.

Studies in the area are very limited, and the strength of these passwords depends in a big part on how easy we want them to be for memorization. Factors such as being easy to memorize and difficulty to crack need to be further researched in order to achieve an accurate conclusion.

5 Vulnerabilities or Attack Vectors

Passwords have a simple task, to "ensure admission or acceptance" [28], however they are not very practical for humans, and their strength – discussed in section 4 – is questionable in multiple instances. Moreover, there exists a considerable lack of research on how hard it would be to crack graphical passwords, and as a result of their insufficient use in practice it is difficult to posit vulnerabilities or attack vectors [29]. Nonetheless, we have researched within the available literature and found that passwords suffer fundamentally from two types of attacks; guessing and capture attacks.

5.1 PassFaces$^{\text{TM}}$ Vulnerabilities or Attack Vectors

PassFaces$^{\text{TM}}$ is a commercial system that is highly secure according to their website [11], where they emphasize the fact that the system uses two factor, two way, and cognometric authentication. Despite the fact that their opinion might be biased, Tari et al. [30] concluded that – if not using a mouse – PassFaces$^{\text{TM}}$ is considerably more secure than text passwords or PINs to shoulder-surfing [30]. Furthermore, Dunphy et al. [31] studied if it would be possible to log in based on the description of the faces and in fact that was case in 8% of attempts. Moreover, Dunphy et al. [31] studied the case where the random faces were similar to the one described and he found that in fact "participants were less likely" [32] to guess if that was the case. Also, Dunphy et al. [31] introduced and tested eye-gaze as input which turned out to improve participants' capacity to enter their passwords.

5.2 GrIDsure$^{\text{TM}}$ Vulnerabilities or Attack Vectors

GrIDsure$^{\text{TM}}$ [12] is propitious to shoulder-surfing attacks because recurrently the complete grid can be seen on the screen while it is being inserted. Brostoff, Inglesant, and Sasse argued that the GrIDsure scheme "might be expected to enhance security over textual passwords and PINs" [21] by encouraging the user to have a more secure behaviour, by reducing the risk of interception and by reducing the possibility of a guessing or brute-force attack. This position is defended by Weber [33] in the paper "The Statistical Security of GrIDsure" were he affirms that the GrIDsure sheme is "much more secure than traditional PINs", above all against shoulder-surfing. Brostoff et al. [21] also discovered that users chose predictable patterns – if not instructed otherwise – and that is in fact a serious vulnerability that might be exploited by attackers.

In contrast, Bond [22] argued that "GrIDsure is no more secure than a PIN", mainly against phishing or man-in-the-middle. Furthermore, GrIDsure "does apparently provide protection against keyboard logging viruses, worms and trojans" [22].

GrIDsure's authentication system stands is obscure considering that studies thus far have been inconclusive because they are flawed or were taken out of context [22]. Bond concludes that his initial study indicates "further weaknesses" and that the development of proper attack methodologies will only be economically feasible if the system gains a large market share.

5.3 PassPoints Vulnerabilities or Attack Vectors

PassPoints stores the passwords in hashed form which prevents capture attacks; has large password space, specially when compared with passwords that are alphanumeric and recognition-based graphical passwords [13]. Furthermore, Davis et al. [34] argues that there exists low entropy if human faces are used; commonly due to the fact that users choose faces that are similar to themselves.

In contrast, users might be seduced by objects that have a peculiar color, size or placement [13].

5.4 Overall Vulnerabilities or Attack Vectors

Davis et al. [34] argued that giving the user the possibility to choose their own passwords will lead to "predictable patterns that may exploited by attackers" [14], these predictability problems affect Passfaces^{TM} and PassPoints. Furthermore, the freedom to set a password will – as studied by Florencio [35] – lead users to reuse the same password for multiple accounts. Moreover, Adams et al. [15] argued that users develop "unsafe practices" in order to overcome the difficulty of remembering passwords.

Brute force search is harder against graphical passwords because programs would have to generate mouse motion to reproduce human input, which is exceptionally challenging [29]. Dictionary attacks are impractical but not impossible, however further research is required in this area. Guessing is where graphical passwords are more fragile because of their predictability, Davist et al. [34] concluded that on the Passface technique users frequently pick weak and predictable graphical passwords. Spyware, in spite of minor exceptions [36, 37], is impractical, and techniques such as key listening or key logging would not be possible to crack graphical passwords. Shoulder surfing along with guessing is where graphical passwords are more vulnerable, none of the techniques analysed in this report are designed to resist shoulder-surfing. Finally in terms of social engineering, graphical passwords are fairly strong and it would not be feasible to give the password over the phone, moreover, creating a phishing web site would also be a daunting task for attackers.

6 Conclusion

In terms of memory recall the main issue users faced was the difculty in learning their passwords [13], this obstacle can conceivably be overcome when the users are more familiar with the concept of graphical passwords. Moreover, the retention of the graphical password in a six week period was identical to alphanumeric users [13]. Furthermore, it is very important to research the retention of graphical passwords in the case where users have several accounts.

In terms of strength, graphical passwords seem to be reasonably strong compared to text-based passwords; especially if we consider how users pick their text-based passwords in real life. It is difficult however to compare and contrast the techniques reviewed in this report due to the lack of research.

In terms of security, and for an apples-to-apples comparison, one needs to be able to exhaustively measure the characteristics of each system. It is not possible to compare different authentication methods as if they were the same. Graphical passwords seem to be less vulnerable to brute force, dictionary, spyware and social engineering attacks, but in contrast, more vulnerable to guessing and shoulder-surfing attacks. Further research is needed into how users would use graphical passwords in real life. It is not sufficient or acceptable to conduct a few number of studies and make assumptions about how the users would behave without supervision.

Overall, graphical passwords although in need of more research seem to be a possible alternative to text-based passwords in the near future. Especially due to their increased security and ease of memorization.

Bibliography

[1] Z. Zheng, X. Liu, L. Yin, and Z. Liu. A hybrid password authentication scheme based on shape and text. *Journal of computers*, 5(5):765–772, 2010.

[2] L.D. Paulson. Taking a graphical approach to the password. *Computer*, 35(7):19–19, 2002.

[3] H. Gao, X. Liu, R. Dai, S. Wang, and X. Chang. Analysis and evaluation of the colorlogin graphical password scheme. In *Image and Graphics, 2009. ICIG'09. Fifth International Conference on*, pages 722–727. IEEE, 2009.

[4] A. Paivio, TB Rogers, and P.C. Smythe. Why are pictures easier to recall than words? *Psychonomic Science*, 1968.

[5] G.H. Bower, M.B. Karlin, and A. Dueck. Comprehension and memory for pictures. *Memory & Cognition*, 3(2):216–220, 1975.

[6] R.N. Shepard. Recognition memory for words, sentences, and pictures1. *Journal of Verbal Learning and Verbal Behavior*, 6(1):156–163, 1967.

[7] A. Paivio. Dual coding theory: Retrospect and current status. *Canadian Journal of Psychology/Revue canadienne de psychologie*, 45(3):255, 1991.

[8] J.M. Clark and A. Paivio. Dual coding theory and education. *Educational psychology review*, 3(3):149–210, 1991.

[9] I. Jermyn, A. Mayer, F. Monrose, M.K. Reiter, and A.D. Rubin. The design and analysis of graphical passwords. In *Proceedings of the 8th USENIX Security Symposium*, pages 1–14. Washington DC, 1999.

[10] J.G.W. Raaijmakers and R.M. Shiffrin. Models for recall and recognition. *Annual review of psychology*, 43:205–234, 1992.

[11] Passfaces Corporation. Passfaces: Two factor authentication for the enterprise, 2012. [Online; accessed 03-March-2012].

[12] GrIDsure. Gridsure - pattern authentication, 2012. [Online; accessed 03-March-2012].

[13] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, and N. Memon. Passpoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, 63(1):102–127, 2005.

[14] R. Biddle, S. Chiasson, and PC Van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys*, 44(4):2012, 2011.

[15] A. Adams and M.A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[16] E. Tulving and M.J. Watkins. Continuity between recall and recognition. *The American Journal of Psychology*, pages 739–748, 1973.

[17] E.C. Carterette, M.P. Friedman, J.L. Miller, and P.D. Eimas. *Handbook of Perception and Cognition*. Academic Press, 1994.

[18] D. Weinshall. Cognitive authentication schemes safe against spyware. In *Security and Privacy, 2006 IEEE Symposium on*, pages 6–pp. IEEE, 2006.

[19] T. Valentine. An evaluation of the passface personal authentication system. Technical report, Technical Report, Goldsmiths College, University of London, 1998.

[20] K.M. Everitt, T. Bragin, J. Fogarty, and T. Kohno. A comprehensive study of frequency, interference, and training of multiple graphical passwords. In *Proceedings of the 27th international conference on Human factors in computing systems*, pages 889–898. ACM, 2009.

[21] S. Brostoff, P. Inglesant, and M.A. Sasse. Evaluating the usability and security of a graphical one-time pin system. In *BCS Conf. on Human Computer Interaction (British HCI)*, 2010.

[22] M. Bond. Comments on gridsure authentication. *Retrieved on August*, 25:2010, 2008.

[23] D. Nali and J. Thorpe. Analyzing user choice in graphical passwords. *School of Computer Science, Carleton University, Tech. Rep. TR-04-01*, 2004.

[24] F.I. Craik and J.M. McDowd. Age differences in recall and recognition. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 13(3):474, 1987.

[25] J.T. Wixted. The psychology and neuroscience of forgetting. *Annu. Rev. Psychol.*, 55:235–269, 2004.

[26] M. Shahid and M.A. Qadeer. Novel scheme for securing passwords. In *Digital Ecosystems and Technologies, 2009. DEST'09. 3rd IEEE International Conference on*, pages 223–227. IEEE, 2009.

[27] R. Jhawar, P. Inglesant, N. Courtois, and M.A. Sasse. Make mine a quadruple: Strengthening the security of graphical one-time pin authentication. In *Network and System Security (NSS), 2011 5th International Conference on*, pages 81–88. IEEE, 2011.

[28] Dictionary.com. Password — define password at dictionary.com, 2012. [Online; accessed 03-March-2012].

[29] X. Suo, Y. Zhu, and G.S. Owen. Graphical passwords: A survey. In *Computer Security Applications Conference, 21st Annual*, pages 10–pp. IEEE, 2005.

[30] F. Tari, A. Ozok, and S.H. Holden. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *Proceedings of the second symposium on Usable privacy and security*, pages 56–66. ACM, 2006.

[31] P. Dunphy, J. Nicholson, and P. Olivier. Securing passfaces for description. In *Proceedings of the 4th symposium on Usable privacy and security*, pages 24–35. ACM, 2008.

[32] R. Biddle, S. Chiasson, and P.C. van Oorschot. Graphical passwords: Learning from the first generation. Technical report, Technical Report TR-09-09, School of Computer Science, Carleton University, 2009.

[33] R. Weber. The statistical security of gridsure. *Retrieved August*, 21:2010, 2006.

[34] D. Davis, F. Monrose, and M.K. Reiter. On user choice in graphical password schemes. In *Proceedings of the 13th conference on USENIX Security Symposium-Volume 13*, pages 11–11. USENIX Association, 2004.

[35] D. Florencio and C. Herley. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web*, pages 657–666. ACM, 2007.

[36] D. Hong, S. Man, B. Hawes, and M. Mathews. A graphical password scheme strongly resistant to spyware. In *Proceedings of International conference on security and management. Las Vergas, NV*, 2004.

[37] S. Wiedenbeck, J. Waters, L. Sobrado, and J.C. Birget. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proceedings of the working conference on Advanced visual interfaces*, pages 177–184. ACM, 2006.