WORLD ORGANIZATION OF APPLIED SCIENCES JOURNALS

International Journal of Information Technology and Applied Sciences
ISSN (2709-2208)
Int. J. Inf. Tec. App. Sci. 3, No.4 (December-2021)
https://doi.org/10.52502/ijitas.v3i4.201

Attacks on Graphical Password: A Study on Defense Mechanisms and Limitations

Indrani Roy[1], Ajmerry Hossain[2], and Sarker T. Ahmed Rumee[3]

[1,2,3] *Department of Computer Science and Engineering, University of Dhaka, Dhaka-1000, Bangladesh*

Abstract: User authentication is mostly reliant on password-based based verification. Users generally used text-based passwords, which are user-friendly but often predictable and vulnerable to some common attacks. To overcome these shortcomings, graphical authentication methods have emerged. Here, users choose a sequence of images as passwords. Though such methods help users to better remember their passwords, they too suffer from attacks seen in the case of textual passwords. This paper presents a comprehensive summary of the vulnerabilities state of the art graphical password schemes against the following well-known attacks - Dictionary, Guessing, Brute force, Shoulder surfing, Spyware, and Social engineering. We believe the findings of this study can help researchers design more secure graphical password schemes making them more usable and a realistic replacement for text-based passwords.

Keywords: Graphical passwords, Attacks, Defenses, Security, User authentication.

1. Introduction

User authentication has a major role in ensuring the security of any system. Generally, user authentication schemes provide an interface for users to enter their username and password. This is widely adopted and still the de-facto standard in ensuring the authenticity of users. However, text-based passwords also suffer from some major shortcomings. Users often choose short and easily predictable passwords susceptible to a well-known attack: dictionary, brute force, guessing attacks, etc. A study done by Xiaoyuan et al. discovered that 80% of the textual password can easily be cracked in a sample network within 30 seconds [1].

Graphical passwords came into prominence to counter some of these limitations and mostly work as an additional layer of security over traditional text-based passwords. Renaud [2] and Herley et al. [3] were one of the first to discuss the possibility of using graphical interfaces for authentication purposes. Various psychological studies on the memorability of graphical objects [4, 5, 6, 7] confirmed that people can easily recognize pictures, geometrical shapes patterns, colors, textures - making graphical passwords a strong tool for user authentication.

With all its benefits, graphical passwords are not immune to attacks. Here, the vulnerability arises from the same factors that affect the textual passwords: easily guessable or too simple choices in the construction of passwords.

This paper presents a comprehensive study of various defense mechanisms to guard against such attacks on graphical authentication schemes and their major limitations. The findings of this paper will help researchers to come up with strategies and policies that can make graphical passwords more usable and secure.

2. Graphical Password Schemes

The graphical password authentication methods can be classified into broadly three categories – Recognition based, Recall Based and others combining both techniques.

A. Regonition Based

In this technique, the user needs to choose the correct image (image chosen as the password during registration) from a set of given images. Passface [3], Déjà vu [21], etc. are examples of recognition-based methods.

B. Recall Password

In Recall based method, the user needs to recollect the password based on memory and not with any kind of clue from the system. Such techniques can be further divided into two categories: Pure recall-based (no hint at all) and Cued recall-based (using some hints to aid recall).

For example, Grid selection [3], Das [21], etc. are pure recall-based techniques. On the other hand, Blonder [25], Pass point [21], etc. are well-known cued recall-based techniques.

C. *Hybrid Technique*

As the name suggests, these techniques ensemble the benefits of both recognition and recall-based methods and often have the better applicability in terms of usability perspective. Few notable work applying hybrid technique are - Jiminy, S3pas and Cas [24], etc.

3. ATTACKS ON GRAPHICAL PASSWORD

Commonly seen attacks to break the security of graphical passwords are briefly discussed below:

A. *Brute Force Attack*

The success of this attack depends on the set of predefined values. Here, a complete key search is done, an attacker guesses (tries) all possible combinations to crack the password. The only way to prevent this attack is to have a larger password space.

B. *Dictionary attack*

Here a dictionary (list of words) is exhaustively searched to break the password. Unlike brute force attacks, this technique employs a systematic key search that considers possibilities most likely to succeed. However, its success guarantee is not the same as in brute force search. scheme is completely resistant to a dictionary attack.

C. *Guessing attack*

Guessing attack, as its name suggests, tries to crack a password based on some predetermined knowledge about the possibilities. People often include personal information like a family name, date of birth, job position, etc. An attacker launch guessing attacks by somehow predicting that information. Although success depends on the quality of guess, such attacks are still a major threat taking into consideration the security unaware user behavior and choice.

D. *Spyware*

This attack happens through malicious software installed on the user’s computer. It is generally done via a key logger or key listener. The goal of this attack is to collect user information and disclose the information. In this attack, the attacker wants to get information and valuable data from the user’s computer by tracking key pressing and mouse clicking events.

Unfortunately, graphical password is very much vulnerable to this type of attacks and unable to escape from this kind of attack.

E. *Shoulder Surfing*

Sometimes a password can be leaked if an intruder can peek into it while using it. These attacks, known as shoulder surfing attacks, are mostly possible when a user is operating in a public space. Users generally focus on accessing the desired system/services while someone who is close by can become a potential attacker in this regard. Small authentication credentials such as ATM or account pins (generally 4 digits) or smartphone unlock patterns/pins are more prone to such attacks.

F. *Social Engineering*

In the context of information security, Social engineering attacks remain a concern because it is the psychological manipulation of cyber attackers. This attack is also known as description attack where attacker gains private data or information from user interaction. Here, attacker doesn’t use any electronic media, they just only use human intelligence to get the information. It is a confidence trick for the purpose of information gathering, fraud, or system access which can break standard security systems easily.

4. CURRENT DEFENCES AND LIMITATIONS

There has been significant attention from the research community to develop more sure yet usable graphical password authentication methods over the years.

This section lists few of the prominent graphical authentication methods/systems described in the literature along with their capability against the common security attacks described in section 3.

Table I summarizes the findings of this study. Here we list the state of the art graphical password schemes and their status in terms of capability to withstand attacks. If a certain method is resistant to an attack, it is shown with a (✓) sign. If it is vulnerable, then the symbol (*X*) is used. On the other hand, for those methods there is no mention or study describing their behaviour against a particular attack it is mentioned as unknown (-).

5. CONCLUSION

This paper presents a comprehensive study on how different graphical password schemes react to traditional attacks which are very common in case of text-based passwords. The results found give us important insight on the state of the art of graphical authentication methods, their capabilities and limitations.

Findings of this paper can be helpful in designing better policies and methodologies to design more secure graphical password schemes.

TABLE I : Attacks on Graphical Password Schemes and Defences

X = Vulnerable to attack , ✓= Resistant to attack, " -" = Not mentioned/found

	Dictionary	Guessing	Brute Force	Shoulder Surfing	Spyware	Social Engineering
Recognition Based Methods						
Déjà vu [21]	✓	X	X	X	✓	✓
Passface [3]	X	X	X	X	✓	X
Movable Frame [8]	X	X	X	✓	✓	X
Picture password [9]	-	-	X	X	X	X
Triangle Scheme [8]	✓	X	X	✓	X	✓
WIW [23]	-	-	-	X	-	-
Story [21]	-	X	X	X	-	-
Convex Hull Click (CHC) [29]	-	-	-	✓	-	-
GPI [24]	✓	X	-	X	✓	✓
Select-to spawn [15]	-	-	✓	-	-	-
Watermarking Technique [16]	✓	-	-	✓	-	-
Weinshall [14]	✓	-	-	X	✓	✓
Color Login [13]	-	-	-	✓	✓	-
GUABRR [12]	✓	✓	✓	✓	✓	-
Jetafida [11]	-	X	-	X	-	-
ImagePass [29]	-	✓	-	-	✓	-
Wang et al. Scheme [10]	-	-	-	-	✓	-
Intersection Scheme [8]	-	-	✓	-	-	-
Dynamic Block-style [8]	-	-	✓	✓	-	-
Recall Based						
Das [21]	✓	✓	X	✓	X	X
Pass Shapes [17]	✓	X	X	X	✓	X
PassMap [23]	X	-	✓	✓	X	X
PassDoodle [19]	-	-	X	-	-	-
Grid Selection [18]	-	-	-	✓	-	-
QDAS [20]	-	-	X	-	-	-
Syukri Algorithm [21]	✓	✓	X	✓	X	X
Blonder's Scheme [25]	X	✓	✓	✓	X	X
Passlogix v-Go [22]	-	✓	✓	✓	-	-
Visky SFR [25]	X	-	✓	✓	X	X
PassPoints [21]	X	✓	✓	✓	X	X
Background DAS (BDAS) [23]	-	X	-	-	X	X
PassBlot [28]	✓	-	✓	-	-	-
Hybrid Schemes						
JIMINY [24]	✓	X	-	X	✓	✓
S3PAS [24]	X	X	-	✓	✓	-
CAS [24]	✓	X	-	X	✓	-
PASSHANDS [24]	✓	X	-	✓	✓	-
CaRP [26]	✓	✓	-	-	-	-
CDS [31]	-	-	-	✓	-	-
Vibration-And-Pattern (VAP) [30]	-	-	✓	✓	-	-
RAYS' SCHEME [25]	✓	-	✓	✓	-	-

REFERENCES

[1] Al-Ameen, M. N., Wright, M., & Scielzo, S. (2015, April). Towards making random passwords memorable: Leveraging users' cognitive ability through multiple cues. In Proceedings of the 33rd Annual ACM Conference on Human Factors in computing Systems (pp.2315-2324).

[2] Walanjkar, D. D., & Nandedkar, V. (2014). User authentication using graphical password scheme: a more secure approach using Mobile Interface. International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization), Vols, 2(12).

[3] Suo, X., Zhu, Y., & Owen, G. S. (2005, December). Graphical passwords: A survey. In 21st Annual Computer Security Applications Conference (ACSAC'05) (pp. 10-pp). IEEE.

[4] OLUKAYODE, O. A., ITHNIN, N., & OGUNNUSI, O. S. (2014). MEMORABILITY RATES OF GRAPHICAL PASSWORD SCHEMES. Journal of Theoretical & Applied Information Technology, 66(1).

[5] Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR), 44(4), 1-41.

[6] Al-Ameen, M. N., Fatema, K., Wright, M., & Scielzo, S. (2015). The impact of cues and user interaction on the memorability of system-assigned recognition-based graphical passwords. In Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015) (pp. 185-196).

[7] Tidke, M. S., Khan, M. N., & Balpande, M. S. (2015). Password Authentication Using Text and Colors. Computer Engneering, Rtm Nagpur Univer sity, Miet Bhandara.

[8] Sobrado, L. (2002). Graphical passwords. The Rutgers Scholar, an electronic Bulletin for undergraduate research.

[9] Jansen, W., Gavrila, S. I., Korolev, V., Ayers, R. P., & Swanstrom, R. (2003). Picture password: a visual login technique for mobile devices. UMBC Student Collection.

[10] Wang, L., Chang, X., Ren, Z., Gao, H., Liu, X., & Aickelin, U. (2010, April). Against spyware using CAPTCHA in graphical password scheme. In 2010 24th IEEE International Conference on Advanced Information Networking and Applications (pp. 760-767). IEEE.

[11] Eljetlawi, A. M., & Ithnin, N. (2008, December). Graphical password: Prototype usability survey. In 2008 International Conference on Advanced Computer Theory and Engineering (pp. 351-355). IEEE.

[12] Eljetlawi, A. M. (2008). Study and develop a new graphical password system (Doctoral dissertation, Universiti Teknologi Malaysia).

[13] Gao, H., Liu, X., Dai, R., Wang, S., & Chang, X. (2009, September). Analysis and evaluation of the colorlogin graphical password scheme. In 2009 Fifth International Conference on Image and Graphics (pp. 722-727). IEEE.

[14] Golle, P., & Wagner, D. (2007, May). Cryptanalysis of a cognitive authentication scheme. In 2007 IEEE Symposium on Security and Privacy (SP'07) (pp. 66-70). IEEE.

[15] Shivaprasad, G. (2019). Research and development of user authentication using graphical passwords: A prospective methodology. International Journal of Innovative Technology and Exploring Engineering, 8(9 Special Issue 3), 385-390.

[16] Towhidi, F., Manaf, A. A., Daud, S. M., & Lashkari, A. H. (2011). The knowledge based authentication attacks. In Proceedings of the International Conference on Security and Management (SAM) (p. 1).

[17] Weiss, R., & De Luca, A. (2008, October). PassShapes: utilizing stroke based authentication to increase password memorability. In Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges (pp. 383-392).

[18] Thorpe, J., & Van Oorschot, P. C. (2004, December). Towards secure design choices for implementing graphical passwords. In 20th Annual Computer Security Applications Conference (pp. 50-60). IEEE.

[19] Varenhorst, C., Kleek, M. V., & Rudolph, L. (2004). Passdoodles: A lightweight authentication method. Research Science Institute, 1-11.

[20] Lin, D., Dunphy, P., Olivier, P., & Yan, J. (2007, July). Graphical passwords & qualitative spatial relations. In Proceedings of the 3rd symposium on Usable privacy and security (pp. 161-162).

[21] Gao, H., Liu, X., Wang, S., Liu, H., & Dai, R. (2009, December). Design and analysis of a graphical password scheme. In 2009 Fourth International Conference on Innovative Computing, Information and Control (ICICIC) (pp. 675-678). IEEE

[22] Passlogix graphical password system, www.passlogix.com [Last Visited on 01/11/21].

[23] Ramanan, S., & Bindhu, J. S. (2014). A survey on different graphical password authentication techniques. International journal of innovative research in computer and communication engineering, 2(12), 7594-7602.

[24] Hafiz, M. D., Abdullah, A. H., Ithnin, N., & Mammi, H. K. (2008, May). Towards identifying usability and security features of graphical password in knowledge based authentication technique. In 2008 Second Asia International Conference on Modelling & Simulation (AMS) (pp. 396-403). IEEE.

[25] Ray, P. P. (2012). Ray's scheme: Graphical password based hybrid authentication system for smart hand held devices. Journal of Information engineering and Applications, 2(2), 1-11.

[26] Manasa, S., Rajendra, C., & Rao, G. V. (2015). Captcha as Graphical Passwords (CaRP)-A Novel Security Approach Based on Hard AI Problems. International Journal of Advanced Engineering and Global Technology, 3(08).

[27] Shammee, T. I., Akter, T., Mou, M., Chowdhury, F., & Ferdous, M. S. (2020). A Systematic Literature Review of Graphical Password Schemes. J. Comput. Sci. Eng, 14, 163-185.

[28] Khodadadi, T., Islam, A. M., Baharun, S., & Komaki, S. (2016). Evaluation of recognition-based graphical password schemes in terms of usability and security attributes. International Journal of Electrical and Computer Engineering, 6(6), 2939.

[29] Azad, S., Rahman, M., Ranak, M. N., Ruhee, B. K., Nisa, N. N., Kabir, N., ... & Zain, J. M. (2017). VAP code: A secure graphical password for smart devices. Computers & Electrical Engineering, 59, 99-109.

[30] Azad, S., Rahman, M., Ranak, M. N., Ruhee, B. K., Nisa, N. N., Kabir, N., ... & Zain, J. M. (2017). VAP code: A secure graphical password for smart devices. Computers & Electrical Engineering, 59, 99-109.

[31] Gao, H., Ren, Z., Chang, X., Liu, X., & Aickelin, U. (2010, October). A new graphical password scheme resistant to shoulder-surfing. In 2010 International Conference on Cyberworlds (pp. 194-199). IEEE.