An Investigation of Social Engineering Techniques towards Graphical Password Authentication

[Naser Marwan Oshrok Laban & Mohd Zalisham Jali]

Abstract*—Recently, social engineering has been considered as one of the main processes to break through the information security. Social engineering technique is the way to get unauthorized information and penetrating accounts through the use of non-technical methods rely on the skills of the hacker in the ability to deceive others and persuade them to get as much information. Nowadays, social engineering techniques are considered the most ways that are used to attack and steal the information all over the world, for that it is becoming necessary to study this kind of attacks and find methods that protect the information from the attacks such as graphical password. The main aim of this paper is to thoroughly explain social engineering methods. In addition, the paper will also present a study conducted to compare the graphical password types (click-based and choice-based graphical password) towards passwords guessing, a branch of social engineering methods. To achieve this goal a survey was conducted by distributing a questionnaire to 50 participants. The data were analyzed via SPSS. Results show that choice-based graphical passwords can resist the attacks more than a click-based graphical passwords.

***Keywords*—graphical passwords, social engineering authentication, knowledge-based.**

I. INTRODUCTION

Nowadays, there are many means to attack and steal the information; one of these ways is using social engineering technique. It is becoming essential to find techniques that protect the information from the attacks; since the information can be used by fraudsters, or it can be used as a way to make scammers seem legitimate [1].

One of the fastest growing crimes is identity fraud. Using personal information; it includes bank account numbers, passwords, name and address. However, personal information about when you were born, when you graduated from high school, your pet’s name and other information can lead to fraudsters being able to guess your username and passwords at financial institutions, and get access to your accounts. The personal information can also be useful to scammers [1].

Social engineering has been used to illustrate a number of attacks ranging from widespread phishing for identity information; several researchers try to identify the Social engineering attacks. The term ‘social engineering’ was used in the first by the hacker and it is a common expression for deception people into helping an attacker to contact a target system [2].

Social engineering is widely used by the attackers since it is the easiest way to obtain the access to confidential information or carry out other security-related attacks on information systems [3].

Harl [4] defined the social engineering as “the art and science of getting people to comply your wishes”. Social engineering is the way to get unauthorized information and penetrating accounts through the use of non-technical methods rely on the skills of her employer in the ability to deceive others and persuade them to get as much information [1].

One of the ways that is used to protect the information from being stolen or the attacks is using the graphical password. The graphical passwords have been proposed as an alternative to text passwords in applications; it’s based on graphics and mouse or stylus entry. Graphical passwords have various type, namely; choice-based graphical password, click-based graphical password and draw based graphical password [5].

The password is the most commonly used method for identifying users in computer or communication systems as text password; it is a secret word or characters used for the user’s authentication and identity to gain access to resources. But, it is easy to guess and it is vulnerable to attack by dictionary attack and brute attacks, the graphical password can be used as a solution [6], [7].

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA) [7]. A graphical password is easier than a text-based password for most people to remember.

Naser Marwan A.Razzaq Oshrok Laban
Universiti Science Islam of Malaysia
Malaysia

Mohd Zalisham Jali.
Universiti Science Islam of Malaysia
Malaysia

Users can use the graphical password by several techniques; draw a simple picture in 2d grid, drawing a signature by using the mouse, click on various points on a picture with a specific sequence to create a password or pick several pictures out of many choices. The security of the system by using the graphical password is very high. On the other hand, the disadvantages for the using of graphical password that the registration and log in process takes a long time and require much more storage space [6], [7].

Most of the researchers [9], [10], [11] agree that the traditional passwords are easy to penetrate by all kinds of attack methods such as; brute force, dictionary, guessing, spyware and loggers, shoulder surfing and social engineering attacks.

The aim of this paper is to thoroughly explain social engineering methods. In addition, the paper also presents a study conducted to compare the click-based and choice-based graphical password towards passwords guessing, a branch of social engineering methods.

This paper is arranged as follow; section 2 discusses the related work in social engineering techniques and graphical passwords, section 3 illustrates the paper methodology to collect the data, section 3 explains the results and discussion. Finally, section 4 presents a conclusion.

II. RELATED WORKS

This section discusses the literature review that related to social engineering techniques and graphical passwords.

A. *Social Engineering Techniques*

Social engineering is a process that tries to obtain confidential information. It is a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking people into breaking normal security procedures [9], [12]. Social engineering involves several methods and techniques to access the information and penetrate accounts [14].

1- Attention-grabbing subject: One of the most common ways is to try to attract the victim by sending an email to his computer and tell him, for example, the need to upgrade software by clicking on the link, this technique conducted after the attacker obtains the victim confidence [15].

2- Trusted e-mail source**:** Try to use e-mail by relying on a trusted name and impersonate, this source on the sender whom this method is easy to use and does not require effort and many steps to get the confidence of the victim [15].

3- Confidence-building: It based on obtain the confidence of the victims. The information is being given to increase the victim confidence, and then ask them by a massage to do something [15], [16].

4- Trusted domain: By exploitation of the confidence; in this case, the attackers exploit the confidence of the reader of the site and send requests to the reader to follow the link on the page. This link actually is referring to a web page not related to the organization [15], [17].

5- Generic Sender: This method is by withholding information about the sender and the development of a generic name. It is best to increase the confidence put the name of the same person to achieve the connection [15].

6-Reverse Social Engineering (RSE): This method is based on the work of propaganda for the engineer as a social security or technical adviser. This is done through several ways, for example, sending e-mails announce the services provided by or through the business cards at this stage, the social engineer finds a security problem for the company, which will connect to it on the grounds that an expert or security adviser, who in turn tempo damage network connection and access to information and data theft. The attacker at this method gives an impression of fixing a problem [18].

7-Piggy-backing Tactic: This method also stressed in the engineer impersonating social facilities for example; an important person has the right to access to buildings and company information. The attackers can exploit the respect of authority and build relationships with victims to gain their trust and get information [17].

8-Techie Talk Tactic: Based on curiosity of the victim; a lot of penetration testing methods and malicious hackers come from a technical background and technique rather than a psychological background. Accordingly, the technicians when it needs to use social engineering; they are choosing the ways in which they know being technical ways; at this method the attacker convince the victim to do something as give out password [19].

9-A Phishing Attack: Phishing attack based on the greed of the victim by sending email messages by the social engineer from project sites known to the general public, such as banking sites or electronic-commerce sites. The person is asked to visit the site or link and the introduction of private and sensitive information such as bank account and password. To convince the person or the victim must appear on the site, it's true, but in fact, the site was created by the social engineer [14], [20].

10-A Spear Phishing Attack: This method also depend on the greed of the victim, it based on using information by the social engineer such as the person's name or address; this information will be the first step. And then use this information through the victim included in an e-mail to more legitimate ignorance and reliability of the victim. Also this type based on the curiosity [14].

11-A Whaling Attack: This type based on the selection of important people in the organization, such as executives or heads of companies. The information about these persons can be obtained easily from the web sites and then used by the attacker to make an attack. Because of the vast amount of information about managers and high-profile targets, whaling is becoming popular because this information makes it so easy for social engineers to target them in a convincing manner.

12-Vishing (voice phishing) Attack: This is another type of phishing attacks, but this type does not use the Internet and e-mail, it uses the phone by sending voice messages to the victim's phone or send text messages requesting information from unauthorized or resolve an issue by deceiving these people and it depending on obtain the victim trust and confidence [16].

13-Social Networking Site’s Attacks: The social networking sites like Face book, Twitter and other sites. These sites are the best environment for the attackers to hunt people and access to information pertaining to them, such as their interests and their workplaces and many others. The researchers show that, most people trust in the friend requests that come by the social networking sites. It's based on the user's curiosity since user try to make a new relationship and knowing a new people [17].

14-Neuro-linguistic programming (NLP) Attacks: NLP is a psychological tool used by social engineers to manipulate people. This method relies on the ability of an attacker to read the physical language and neurological for people targeted and appears to read the reflexes and the ability to observe behavioural patterns of people, practices, and then exploit all these aspects to gain the trust of the people to get the information.

15-Exploiting the Sex: This way also based on curiosity of the victim to manipulate people to achieve social engineer advantage. In this method the attacker convince the victim by using mutual chemistry which is one of the oldest social engineering tricks in the world [16].

16-Exploiting Humans' Problems: This method by exploiting the psychological side of the victims. The attackers follows the victims to gain the information, while the victims are unconscious (screwed). For example; the attackers exploit their presence in bars and exploitation of the mental state of the persons and the situation of loss of consciousness as a result of drinking then the attacker accesses to information [21].

17-Guessing attack: It is one of the most important ways of the social engineering techniques. It's based on the ability of the attackers to guess the victim password. This method based on exploiting the confidence of the victim to get the personal information and then to guess the password. So, guessing attack is considered one of the social engineering attacks [9].

Social engineering attacks can be classified into a number of distinct classes based on the behaviour and possible impact or severity of damages, it also can be classified based on; human based and computer-based [22]. Based on the literature review Social Engineering Attacks can be classified into four groups depending on the exploitation of one of the weaknesses; The first group consists of the techniques that exploiting the victim's confidence, second group consists of techniques based on greed, third group based on the curiosity and the final group based on the human psychology (Figure 1).

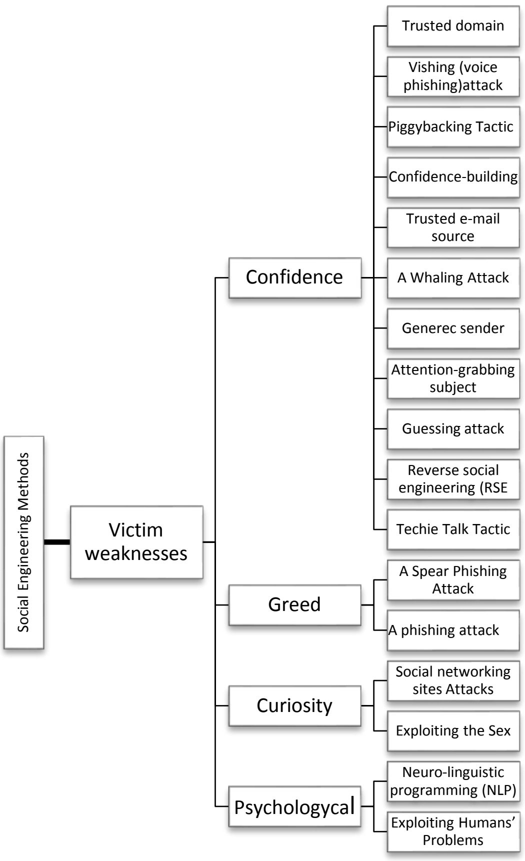

Figure 1. SEM classification.

B. *Traditional password*

In spite of the vast number of options for authentication, traditional passwords remain the most familiar alternative for a number of reasons; traditional passwords are easy and inexpensive to implement, and are familiar to most users. Traditional passwords allow users to authenticate themselves without violating their privacy, as biometrics could, since users can select passwords that do not contain personal information [23].

Traditional passwords are hard to remember and relatively easy to attack; traditional passwords are easy to penetrate by all kinds of attack methods such as; brute force, dictionary, guessing, spyware and loggers, shoulder surfing and social engineering attacks, they based on their results on a laboratory survey to determine the ability of the attackers to predict the passwords [9], [10].

C. *Graphical Passwords*

Graphical passwords (GP) based on utilizing images instead of text. Various kinds of attacks can penetrate the graphical password such as; shoulder surfing attacks and social engineering attacks. Social engineering attacks can guess the user's password by using common personal information [8], [9], [10]. Graphical passwords are three types: click-based graphical password scheme, choice-based graphical password scheme and draw based graphical password scheme [24].

1- Click-based graphical password scheme

Click-based graphical password scheme consists of various click points on a single image or photo. User clicks on any places on an image to construct a password. In order to be authenticated, the user must click within the tolerance in the correct square [13], [25].

2- Choice-based graphical password scheme

Choice-based graphical password consists of different images. To construct this kind of password, the user picks several pictures out of many choices; identify them later in authentication [13].

3- Click Draw-based Graphical Password Scheme

This scheme consists mainly of two steps are; Image selection and Secret drawing. The user draws a simple picture on 2D grid occupied by the picture is stored in the order of drawing. To log in, the user must redraw the password by touching the same grid in the same order [13], [17].

Based on the literature review, this paper summarized the impact of social engineering attacks on both of the graphical password and traditional password as in TABLE 1.

TABLE 1. Graphical and Traditional Password Attacks

Social Engineering attacks	GP	TP
1-Attention-grabbing subject	×	√
2-Trusted e-mail source	√	√
3-Confidence-building	×	√
4-Trusted domain	×	√
5- Generic sender	×	√
6-Reverse social engineering	×	√
7- Piggybacking Tactic:	×	√
8- Techie Talk Tactic:	×	√
9- A phishing attack:	√	√
10- A Spear Phishing Attack:	√	√
11- A Whaling Attack:	×	√
12- Vishing (voice phishing) attack:	×	√
13- Social networking sites Attacks:	×	√
14-Neuro-linguistic programming (NLP) Attacks	×	√
15- Exploiting the Sex:	×	√
16- Exploiting humans' problems	×	√
17-Guessing attacks	√	√
√= yes ×= No		

III. METHODOLOGY

The survey was conducted by using a questionnaire to determine the impact of social engineering attacks against graphical passwords types (choice-based graphical passwords and click-based graphical passwords); since the choice-based graphical password and the click-based graphical password depend on choosing from a specific photo unlike draw-based which creates a new drawing by the users.

A questionnaire was distributed to test the ability of the attackers to guess the passwords, and then a comparative evaluation study was conducted to determine the best graphical password type that can resist the social engineering attacks. Based on the results, a comparative study will be conducted to determine the best kind of graphical password that resists the social engineering attacks.

The questionnaire consists of four parts; the first part is an introduction, it includes the instructions that the participants must follow to answer the questions. The second part is about the participant's information as; name, email, study program (undergraduate or postgraduate), the participants' university and gender. The third part has nine photos (choice-based graphical passwords) (Figure 2). And the fourth part has a photo with various points on it (click-based graphical passwords) (Figure 3).

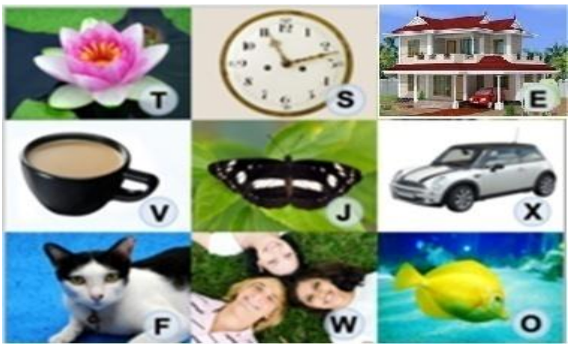

Figure 2. Choice-based graphical passwords.

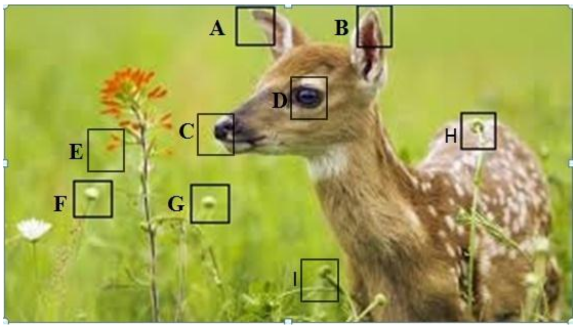

Figure 3. Click-based graphical passwords.

The role of the participants is to guess the needed passwords (choice-based and click-based graphical passwords); each participant has three attempts to guess the needed passwords. Each password consists of five objects with a sequence order. the needed choice-based graphical password is (fish, butterfly, flower, o'clock and house); the participants have to write down the symbol for each object. Therfore, the sequence order of the objects' symbols is; O, J, T, S and E. The needed click-based graphical password is (orange bud, white bud, green bud, nose and eye); the participants have to write down the symbol for each object. Therfore, the sequence order of the objects' symbols is; E, F, G, C and D.

IV. RESULT AND DISCUSSION

In total, this study managed to recruite a total number of 50 participants. Majority of participants were female, where only 16 of the participants were male. 28 of the participants were from USIM and 22 participants from UKM. 37 of the participants were undergraduate students, with 13 were postgraduate students.

In the choice-based graphical password, the frequency of the patterns shows that the most patterns which were used by the participants to guess the needed password was as the following arrange; the most is T (flower), then S (clock), E (house), O (fish), W (faces), X (car), F (cat), V (coffee) and finally J (butterfly) (Figure 4). The choice-based graphical password was guessed by two participants. In the first no one guessed the password, while a participent guessed the password in the second attempt and a participant in the third attempt.

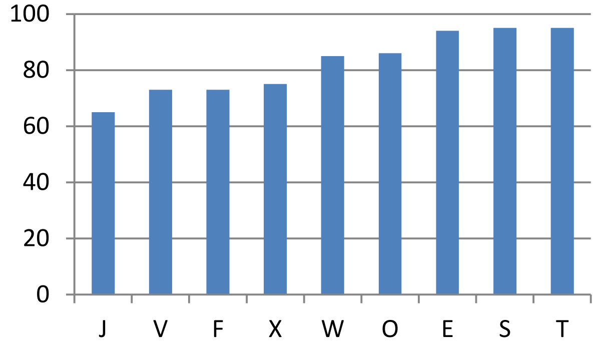

Figure 4. Pattern’s repetition at the choice-based

In the click-based graphical password, the frequency of the patterns shows that the most patterns which were used by the participants to guess the needed password was as the following arrange; the most is D (eye), then C (nose), E (orange bud), A (ear), H (bud), B (left ear), G (bud), F (white bud) and finally, I (branch) (Figure 5). The click-based graphical password was guessed by three participants. A participant guessed the click-based graphical password in the first attempt and two participants guessed the password in the third attempt.

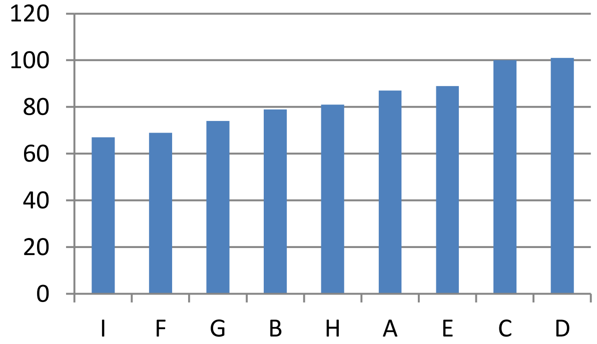

Figure 5. Pattern’s repetition at the click-based

Based on results, the study suggests that both of the graphical password types (choice-based graphical password and click-based graphical passwords) have the ability to resist the attacks. However, the choice-based graphical password is better than click-based graphical passwords in resisting the attacks, since the persons who guessed the password in the click-based graphical password attempts is more than the person who guessed the password in the choice-based graphical password attempts.

V. CONCLUSION

The aim of this paper is to clarify the social engineering methods. In addition, the paper will also present a study conducted to compare the click-based and choice-based graphical password towards passwords guessing, a branch of social engineering methods.

This paper has two main objectives; (a) compare the effect of the social engineering attacks on traditional and graphical passwords and (b) determine the graphical password type that resists the social engineering attacks.

To achieve the first object; secondary data about social engineering attacks, traditional passwords and graphical passwords were collected from the literature review. By comparing the impact of social engineering methods on traditional password and graphical password the result show that the traditional password is easily attacked by all kinds of attacks. A questionnaire survey was used to achieve the second objective; 50 participants of university students fill out the questionnaires. The results show that the choice-based graphical password is better than click-based graphical passwords in resisting the attacks.

These results are satisfied; the choice-based graphical password is more difficult to guess in comparing with the click-based graphical password since there is a vast amount of photos. While, the probability to guess the password in click-based is more since there is a specific photo. This study can be improved by test the effect of social engineering attacks on the three types of graphical password (choice-based, click-based and draw based) to determine the best type that could be used. Another way is by studying the impact of several techniques (social engineering attacks and brute attacks) on the graphical password types.

Acknowledgment

The authors wish to thank participants for participating in this project. This work is part of the master degree.

References

[1] L. A. Gordon and M. P. Loeb, “The economics of information security investment,” ACM Transactions on Information and System Security (TISSEC), vol.5, iss. 4, pp.438-457, 2002.

[2] K. Townsend, “The art of social engineering. Info security, vol. 7, iss.4, pp. 32-35, 2010.

[3] M. Workman, “Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security,” Journal of the American Society for Information Science and Technology, vol. 59, iss. 4, pp.662-674, 2008.

[4] S. Granger, “Social engineering fundamentals,” part I: hacker tactics. Security Focus, December, 18, 2001.

[5] G. E. Blonder, "Graphical password," U.S. Patent vol. 5, pp. 559-961, September 1996.

[6] E. A. Stobert, “Memorability of assigned random graphical passwords,” Carleton University (Canada), UMI Dissertations Publishing, 2011.

[7] D. L. Nelson, “Use of image-based mnemonic techniques to enhance the memorability of user-generated passwords,” California State University (Long Beach), Dissertations Publishing, 2004.

[8] L. Y. Por, and X. T. Lim, “Threats and Future Trend for GSP,” 7th WSEAS Int. Conf. on Applied Computer & Applied Computational Science (ACACOS '08), Hangzhou, China, 2008.

[9] A. H. Lashkari, A. A. Manaf and M. Masrom, “Graphical Password Security Evaluation by Fuzzy AHP,” Proceedings of World Academy of Science, Engineering and Technology. World Academy of Science, Engineering and Technology, 2012.

[10] P. Dunphy, “Usable, Secure and Deployable Graphical Passwords,” Newcastle University PhD Thesis, vol. 1, 2013.

[11] W. Z., Khan, M. Y. Aalsalem and Y. Xiang, “A Graphical Password Based System for Small Mobile Devices,” International Journal of Computer Science Issues (IJCSI), vol. 8, iss. 5, 2011.

[12] E. Stobert, Forget, A. Chiasson, S. van Oorschot P. C. and Biddle R, "Exploring usability effects of increasing security in click-based graphical passwords," Proceedings of the 26th Annual Computer Security Applications Conference. ACM. pp. 79-88, 2010.

[13] P. R. D. Shrikala, M. Deshmukh and A. B, Pawar, "Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme," International Journal of Soft Computing and Engineering (IJSCE), vol. 3, iss. 2, pp. 2231-2307, 2013.

[14] M. Guenther and R. Broadhurst, "Social Engineering and Crime Prevention in Cyberspace," Queensland University of Technology, 2006.

[15] T. Bakhsi, M. Papadaki, and S.M. Furnell, "A Practical Assessment of Social Engineering Vulnerabilities," Proceedings of the second International Symposium on Human Aspects of Information Security & Assurance (HAISA), 2008.

[16] I. Danesh, B.Marco, B. Davide, K. Engin and P. Calton, "Reverse Social Engineering Attacks in Online Social Networks," 8th International Conference; DIMVA 2011, Amsterdam, The Netherlands, July 2011.

[17] A. Chitrey, D. Singh, M. Bag, and V. Singh, "A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model," International Journal of Information & Network Security (IJINS), vol. 1, iss. 2, pp. 45-53, 2012.

[18] R. Nelson, "Methods of Hacking: Social Engineering," the Institute for Systems Research, University of Maryland, 2001.

[19] P. Hunton, "The growing phenomenon of crime and the internet: A cybercrime execution and analysis model," Computer Law & Security Review, vol. 25, iss. 6, pp. 528-535, 2009.

[20] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," Communications of the ACM, vol. 50, iss.10, pp.94-100, 2007.

[21] M. Huber, S. Kowalski, M. Nohlberg and S. Tjoa, "Towards Automating Social Engineering Using Social Networking Sites," Enterprise Distributed Object Computing Conference (EDOC), IEEE International, pp. 267 – 274, 2013.

[22] N. Hoquea, M. H. Bhuyana, , R.C. Baishyaa, D.K. Bhattacharyyaa, J. K. Kalitab, "Network attacks: Taxonomy, tools and systems," Journal of Network and Computer Applications, vol. 40, pp. 307–324, April 2014.

[23] K. Renaud, and J. Ramsay, "Now what was that password again? A more flexible way of identifying and authenticating our seniors," Behaviour & Information Technology, vol. 26, iss. 4, pp. 309-322, 2007.

[24] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot and R. Biddle, "Multiple password interference in text passwords and click-based graphical passwords," In Proceedings of the 16th ACM conference on Computer and communications security, pp. 500-511, 2009.

[25] J. C. Gyorffy, "based Graphical Password Authentication," Department of Electrical and Computer Engineering, University of Alberta, Vol. 10, Iss. 6, pp. 321, Nov 2011.

The authentication based upon choice was resist and superior as compared to the authentication based upon click.