International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878 (UGC Approved, Sr. No. 48096)
Index Copernicus Value (2015): 62.86 | Impact Factor (2015): 3.791

Graphical Passwords – YAGP: A User Study

Rajashree Chaurasia

Department of Computer Engineering, Guru Nanak Dev Institute of Technology, *Sector- 15, Rohini, Delhi, India. Pin-110085*

Abstract: ***Authentication deals with determining whom you are communicating with before revealing sensitive data.One of the most important and widely used schemes in this group is graphical password authentication. Like text-based passwords, these are knowledge-based authentication techniques and are advantageous in effecting human memory using visual information. YAGP – Yet another Graphical Password is one such recall based technique. In this paper, the author presents a user study of YAGP and comments on the findings of the study.***

Keywords: YAGP, Graphical Passwords, Authentication, Password, Security

1. Introduction

As the saying goes – 'A picture is worth a thousand words', graphical authentication schemes have been proposed as a prospective alternative to conventional text-based password schemes.

A graphical password is a secret that a user inputs to a computer with the aid of the computer's graphical input e.g., mouse, stylus, or touch screen and output devices.

Graphical passwords can be categorized according to the memory task involved in remembering and entering the password as recall, recognition, and cued recall techniques. Recall requires that a person remember information without any hints. Recall-based graphical password systems are occasionally referred to as draw metric systems [1] because users recall and reproduce a secret drawing, usually on a plain or grid canvas. YAGP (Yet another graphical password) is one such scheme.

2. YAGP

GAO Et Al. [2] proposed YAGP which is a modification to DAS [3] (Draw-a-Secret) in which nearly correct drawings can be accepted based on Levenshtein distance string matching and trend quadrantsobserving the direction of pen strokes. As a result, a finer grid can be made available to the users.

YAGP inherits the advantages of other graphical password schemes. Moreover, it has its distinctive characteristics including allowing redrawing anywhere on the grid, and analyzing user drawing style.

YAGP involves a grid of 48×64 denser than the 5×5 grid used in DAS and thus offers a larger password space. With such a dense grid, it becomes easy for users to draw long strokes without the restrictions of drawing lines crossing grid intersections and over the grid lines.

YAGP imposes no limitation to the number of strokes. Therefore, YAGP provides a larger password space than most existing graphical password schemes. The user interface for YAGP [2] is given below:

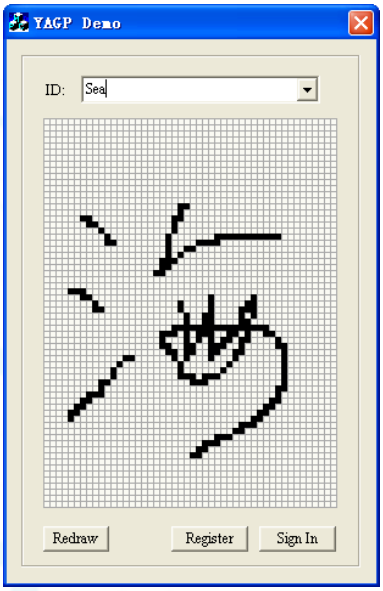

Figure 1: YAGP User Interface

3. Experiment

The author has tested YAGP using the user interface which has been released under the GNU GPL license (found at [4]) by the proponents of the scheme. This tool was developed in C++ as a Windows Application. The grid size of the user interface is 48 x 64. See Figure 1 above.

A. Users recruited for the study

The total number of users involved in the study is 20 (11 males and 9 females). Of these, two users are above the age of 50 years and are inexperienced in using computers and touch-screen devices. Thirteen users are college students (age group between 17-21) of the computer science branch and are fairly experienced in using computers but are only moderately skilled in sketch artistically either with a mouse or stylus. The remaining five participants are lecturers between the age group of 25 and 35 who are experts in the computer science domain as well as better skilled in drawing with a stylus/mouse on a grid.

B. Procedure

In the first phase, all participants were given only basic instructions regarding the purpose of the study. They were shown the UI once and given instructions as to how to use the UI, i.e. how to register and login. In the first trial, users

were not given instructions about the constraints of YAGP, like, the order and number of strokes used to draw the password. This was done to see whether extensive training or instructions are required at the time of registration or signup. Also, it was noted whether any invalid passwords were generated in the process. Each participant was closely observed for the entire duration of the registration and login process. The time of login was also noted for each user.

In the next phase of the study, users were given verbal instructions about the importance of the number of strokes and the order of the strokes used to create the graphical password. Again, the registration procedure was observed carefully. Users were also asked to login once. Both, the login and registration times were noted for each user. Participants were asked to take a short break of 10 minutes and then were requested to login. The number of successful and unsuccessful attempts and time taken to login were recorded. In the third phase, participants were asked to return after one week and re-enter their password to login. The number of successful and unsuccessful attempts and time taken to login were recorded. This gave the author an idea in to the memorability aspects of the scheme. In the fourth phase, users were asked to register with simple passwords with few strokes to see whether the success rate of logins improved. Then they were asked to register with complex passwords to see how the success rate suffers from memorability issues.

Further, to test social engineering attacks, users were asked to describe their passwords to others and then the attackers tried to hack their account. To test shoulder surfing attacks, users were asked to look at the passwords drawn by other users and then try to break their password. The number of successful attempts was noted. This time, attackers only saw the password already drawn on the screen by the other user for 5 seconds. This means that the attackers did not know the number of strokes or the order of strokes entered by the other participant. In the next attempt, attackers were allowed to see one complete login process of another user. Now the attackers were asked to try and break the passwords and the number of successful and unsuccessful attempts was recorded.

Lastly, participants were asked basic questions about their user experience and whether they would like to use such a scheme in future as against text-based password schemes.

4. Results

YAGP is a grid-based and drawing-based technique where user choice is provided to aid memorability and make the system easy and fun to use, just like sketching on a canvas grid. As compared to DAS, YAGP is an improvement in the sense that users can draw their password anywhere on the grid canvas. This gives some amount of freedom to the user and aids memory.

The table below shows gathered data of the first attempt at YAGP registration and login.

Table 1 : First Attempt

First Attempt	Number of Successes	Number of Failures	Average Registration Time (in seconds)	Average Login Time (in seconds) *
Without Instructions	1	19	54	221
With Instructions	14	6	33	36
With Instructions (Simple Password)	17	3	25	27
With Instructions (Complex Password)	11	9	42	167

*: indicates that some users were not able to login at all and the data in the cell indicates the average login times of only the successful users.

When users were not given instructions about the number and order of strokes, only 1 participant was able to login after registration. However, no invalid passwords were generated at the time of registration. With instructions, users understood how the tool actually works and the success rate increased drastically. However, it was also found that to aid memorability, many of the users drew predictable passwords like their initials, simple geometric shapes, items they liked, etc. Not much thought was put into creation of the password according to many participants. This was mainly because the tool does nothing except registration and login. It does not offer any realistic scenario to the user where he/she must protect some personal data from being hacked. When users were specifically told to register with simple passwords, the success rates and time taken to register and login, improved. In contrast, when users were told to register with complex passwords containing more than 5 strokes, the success rates dropped considerably. This shows that YAGP is not as easy to use when users draw complex passwords. However, complex passwords are strong passwords as they contain more number of strokes and these thus offer greater security. It can be seen clearly from the data above that YAGP has some drawbacks as regards its memorability and security. In the next table, the author presents data regarding the second attempt at login after the short 10-minute break given to users.

Table 2 : After 10 minutes

After 10 Minutes	Number of Successes	Number of Failures	Average Login Time (in secs)*
With Instructions	14	6	38
With Instructions (Simple Password)	18	2	41
With Instructions (Complex Password)	9	11	175

*: indicates that some users were not able to login at all and the data in the cell indicates the average login times of only the successful users.

In the next table, the author presents data regarding the second attempt at login after the one-week break given to users.

Table 3: After 1 week

After One Week	Number of Successes	Number of Failures	Average Login Time (in seconds)*
With Instructions	12	8	34
With Instructions (Simple Password)	16	4	37
With Instructions (Complex Password)	8	12	123

*: indicates that some users were not able to login at all and the data in the cell indicates the average login times of only the successful users.

From the data above, it can be seen that memorability is affected in some way after a long period of time is elapsed between logins. It was also noted that to aid memorability, many users (11 out of 20) wrote down their passwords on pieces of paper. This shows that security may be compromised in order to create a complex password. Users said that in order to remember the order of their strokes, they clearly drew the entire password complete with the order and number of strokes on paper to remember them. But it can be seen that users could not exactly remember the grid locations of the strokes and therefore had difficulty re-drawing their password after one week.

To test security features, users were asked to try and break one other user's password (without repetition of users). For social engineering attack, users described their password verbally to the attacker. For shoulder surfing attacks, attackers were first allowed to look at the already-drawn password on the grid canvas for a few seconds and attempt to hack and then allowed to observe one complete login and then attempt to hack. The results are tabulated as follows:

Table 4: Security Aspects (Simple)

Simple Password	Number of Successes	Number of Failures	Average Number of Attempts when successful
Social Engineering Attack	0	20	N/A
Shoulder surfing Attack (1 peek)	0	20	N/A
Shoulder surfing Attack (1 login)	7	13	3

Table 5: Security Aspects (Complex)

Complex Password	Number of Successes	Number of Failures	Average Number of Attempts when successful
Social Engineering Attack	0	20	N/A
Shoulder surfing Attack (1 peek)	0	20	N/A
Shoulder surfing Attack (1 login)	1	19	9

5. Conclusion

The results above show that YAGP is resistant to social engineering attacks of the form when attackers can only gather a description of the password. YAGP is also resistant to shoulder surfing attacks where the attacker does not know of the order and number of strokes in the password. However, when a complete login is observed, the attacker can hack the password of the user in a number of attempts especially if the password is simple. Complex passwords however are still difficult to break but it is not impossible. Thus, such a technique when employed in real scenarios should constrain the number of attempts to three before account lockout occurs. This will prevent a fair amount of shoulder surfing attacks. But when shoulder surfing attackers employ video cameras to record the entire login process, even 1 login observation is enough for the attacker to crack the password and that too in one attempt alone! Such a flaw cannot be ignored in real life situations and a mechanism must be devised to overcome this shortcoming.

Finally, users were asked some questions on user experience and majority of them felt that the system was very easy to use. Most of the users (17 out of 20) reported that the tool appeared like a paint application with a grid to aid memorability. Majority of them (15 out of 20) would like to still stick to text-based password schemes as they feel that the security of YAGP is not a match to their text password counterparts. This was mainly because they felt that the entire password can be seen on the screen as it is drawn and therefore is vulnerable to attacks. This is not the case with text passwords that uses escape characters like * to hide the password being typed in. Also, when asked about how difficult it was to remember 3 different sets of passwords for the user study, most of the participants (11 out of 20) said that they faced a major problem trying to remember which password they used in which set. This increased the number of attempts that they needed to successfully login, thereby increasing the login times. When asked what they feel about the application domain of the current scheme, most (14 out of 20) reported that this technique was better suited for hand-held devices that use a stylus or pen or a touch-screen. They also reported that it was not suitable for those users who suffer from reduced vision or who cannot draw artistically enough, for e.g. those suffering from Parkinson's disorder. Thus, they felt that the technique was more suited to the young and middle aged group with some knowledge or expertise in using such devices.

6. Future Work

The results of the data collected during this research clearly show that YAGP has its advantages as well as its limitations. While it offers an advantage of ease of use at par with that of text passwords, it adds the fun element of sketching your own password to add a visual cue of image memorability as against alphanumeric passwords. Also, the times taken to register and login are almost at par with what we experience when using the text-passwords. This scheme is resistant to many of the security attacks that text-based passwords fall victim to - brute force and dictionary attacks. However, shoulder surfing attack that uses video records of the logins is still an issue that needs to be addressed. Many times, partly due to multiple password interference, users are not able to draw their password accurately. This is an open issue that will need to be considered in future proposals. These and environmental and user-skill related precincts make this scheme a less-frequently chosen option over text-based and biometric authentication. Further research may address these concerns and bring out a technology that is generally applicable to many environments and user-types.

References

[1] A. De Angeli, L. Coventry, G. Johnson and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems." International Journal of Human Computational Studies, 2005.

[2] Gao Et Al. YAGP: Yet another graphical password strategy, Proceedings of the Annual Computer Security Applications Conference (ACSAC), 2008.
[3] A. Jermyn et al., The design and analysis of graphical passwords, Proceedings of the 8th USENIX Security Symposium, 1999.
[4] http://sourceforge.net/projects/yagp-xidian/

Author Profile

Rajashree Chaurasia received her B.Tech. (I.T.) and M.Tech. (I.T.) degrees from Guru Gobind Singh Indraprastha University, Delhi, in 2009 and 2014, respectively. She is a gold medalist in both B.Tech. and M.Tech. as well as UGC NET qualified. She was with Infosys Technologies Ltd. from 2009 to 2011 and thereafter taught at Guru Tegh Bahadur Institute of Technology for a year. She is currently serving as a Lecturer in the Department of Computer Engineering, at Guru Nanak Dev Institute of Technology, Delhi (a Government of NCT of Delhi institution), since 2012.