Multi-level Authentication Scheme using Textual-Graphical Password Method

Akshay Phadake[1] Rohit Mathur[2] Bharat Modi [3] Prof. Sheetal Thakare[4]
[1, 2, 3, 4] Computer Engineering Department
[1, 2, 3 ,4] Bharati Vidyapeeth College of Engineering

Abstract---In Information Technology security plays an integral part which is braced by authentication process. One of the most commonly and traditionally used authentication method is alpha-numeric username and password which are vulnerable to many attacks such as spyware attack, shoulder surfing, brute force etc. To vanquish the cons of traditional methods, graphical and visual passwords have been introduced as possible substitute to text-based scheme. We are in the process of implementing a strong authentication scheme in which text are used along with images and Draw a Secret (DAS) scheme to generate the session password. In addition to this we would make use of an unique SMS service in which the generated session password is being forwarded to the user.

Key words: Textual, Graphical, Visual and DAS, shoulder surfing, Authentication Scheme, Session password.

I. INTRODUCTION

A. *Textual password*

Textual password scheme is one of the most widespread authentication methods used till today's date. It was introduced in the 1960s with some basic rules for better security which user has to consider while setting his password.
Some of them are as follows:

- The password should be at least 8 characters long.
- The password should not be easy to relate to the user.
- The password should not be a word that can be found in dictionary or public dictionary
- Ideally, the user need to combine upper and lower case letters and digits.

But the main threat in this mechanism, as users rarely choose passwords that are both hard to guess and easy to remember. As a result, passwords are often badly selected and therefore more easily guessed or cracked, forgotten, written down, shared with others, infrequently changed and kept the same for multiple systems. So, we can assume that these methods have become very unsafe. Despite their popularity, it is obvious that text passwords can cause serious problems to the users.

1) *Problems with textual password scheme*

- Shoulder Surfing Attack- As the name implies, shoulder surfing is watching over people's shoulders as they process information. Examples include observing the keyboard as a person types his or her password, enters a PIN number, or views personal information. Even though it is usually possible to ensure that there are some people looking over one's shoulder at the time of login, the value of graphical passwords as an alternative to alpha-numeric passwords is enhanced drastically.
- Dictionary Attack-This special type of attack uses words found in the dictionary to check if any words have been used as passwords by the users. Many users use weak passwords which makes it easier for attackers to guess the password.
- Spyware Attack-This attack uses a small application installed on a user's computer which records sensitive data during movement of the mouse or key press. This form of malware secretly stores this information and then reports back to the attacker's system. If the movement is recorded, it is still not accurate in identifying the graphical password. Other information is needed for this type of attack namely window size and position as well as the timing.
- Keylogger Attack-A key logger sometimes called as a keystroke logger or system monitor is a hardware device or small program that monitors each key stroke a user types on a specific keyboard. A key logger program does not require physical access to the user's computer. It can be downloaded on purpose by someone who wants to monitor activity on a particular computer or it can be downloaded unwittingly as spyware and executed as a part of rootkit or remote administration Trojan horse.
- Guessing Attack-Since many users try to select their password based on their personal information like the name of their pets, passport number, family name and so on, the attacker also tries to guess passwords by trying these possible passwords.

To overcome these drawbacks of textual password, graphical password were introduces as the substitute to provide better security. The sophistication of the security provided by graphical password becomes hard to crack, monitor or being hijacked by the hackers.

B. *Graphical passwords*

As we live and communicate in an environment where the visual sense is predominant for most activities, our brains are capable of storing and processing large amounts of graphical information with ease. It is easy to remember faces, places we have visited before or images than to remember the long character passwords. Thus, graphical password schemes provide a way of making more human-friendly passwords while increasing the level of security and also makes dictionary attacks infeasible, partly because of the large password space, but mainly because there are no pre-existing searchable dictionaries for graphical information. It is also hard to perform automated attacks. Whereas we can recognize a person's face in less than a second, computers spend a considerable amount of time processing millions of bytes of information regardless of whether the image is a face, a landscape, or a meaningless shape.

1) S3PAS scheme

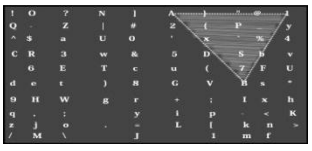
Scalable Shoulder- Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS) was developed to be used in client/server environments as most password authentication systems.S3PAS flawlessly integrates both graphical and textual password methods and provides nearly perfect resistant to shoulder-surfing, spyware attacks and hidden-camera. It can replace or coexist with traditional textual password systems without changing existing user password profiles. Moreover, it is resistant to brute-force attacks through volatile and dynamic session passwords. S3PAS shows significant potential joining the voids between conventional textual password and graphical password.

Shoulder Surfing Resistant Most textual and graphical password schemes are vulnerable to shoulder-surfing. However, our S3PAS scheme offers perfect resistance to shoulder-surfing, hidden camera and spyware. After an attacker observes or records one click on the screen from the user, the attacker can not gain enough information of the users password. This shows that a shoulder-surfing attack is physically infeasible.

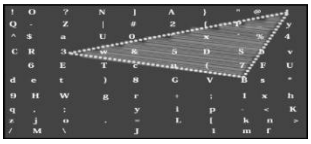
a) S3PAS algorithm

We assume that the user's original password k is "A1B3". Since the length of the password is, |k| = 4, based on the basic click-rule, User has to click four times correctly in the right sequence to be authenticated. The four combinations of password in order are "A1B", "1B3", "B3A" and "3A1". The login procedure consists of the following four steps and is also shown in Figure 1 (a) to (d).

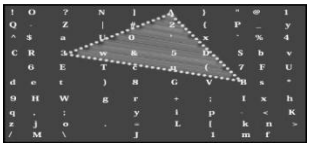
1) User finds her pass-characters "A", "1" and "B", then clicks inside the pass-triangle A1B (e.g., "P").
2) User finds her pass-characters "1", "B" and "3", then clicks inside the pass-triangle 1B3 (e.g., "D").
3) User finds her pass-characters "B", "3" and "A", then clicks inside the pass-triangle B3A (e.g., "5").
4) User finds her pass-characters "3", "A" and "1", then clicks inside the pass-triangle 3A1 (e.g., "2").



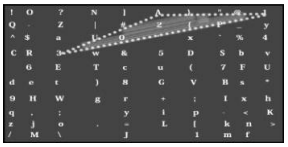
(a) pass-triangle A1B



(b) pass-triangle 1B3



(c) pass-triangle B3A



(d) pass-triangle 3A1

Fig. 1: S3PAS login screen

To prevent Brute-Force attack another module is added to the system which named as Short Message Service (SMS). In this module user want to give his mobile number at the time of registration. After successfully completing above all steps user will get SMS with a unique code without which the user cannot login successfully.

C. Draw A Secret Scheme

We are using a technique; called "Draw a Secret (DAS)".This technique allows the users to draw their unique password. During password creation, a user is asked to draw a simple picture on a 2D grid. The coordinates of the grids used by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated.

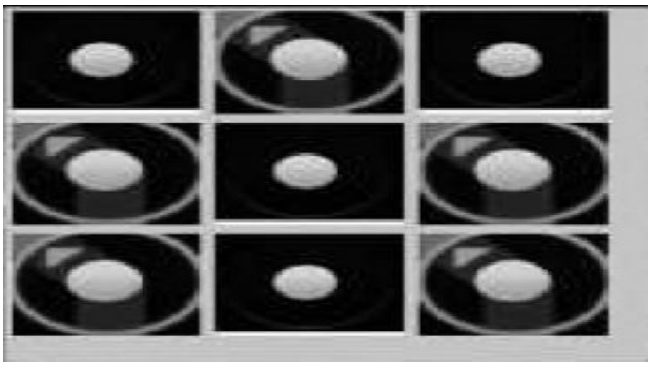


Fig. 2: Draw A Secret Scheme

II. CONCLUSION

We had done the study of various password authentication techniques and carried out our own approach to make the combination of various best authentication system with their advantages at the different levels of authentication. Our proposed approach is resistant to shoulder surfing and strongly resistant to phishing and dictionary attack. S3PAS is scalable in that it seamlessly matches the conventional text-based passwords and can accommodate date various lengths of textual passwords, which requires zero-efforts for users to migrate their existing passwords to S3PAS.The major issues in S3PAS schemes include slightly more complicated and longer login processes. As future work, We plan to design a simplified version of S3PAS with a little lower security level to ease its adoption. As such, we have proposed the idea of utilizing session passwords for authentication. For this purpose, we had made use of all three textual, graphical and DAS techniques.

III. ACKNOWLEDGMENT

Our most sincere appreciation are to all the people who have helped and inspired us throughout the working of this project. Firstly we are thankful to our principle Dr. M. Z. Shaikh for his help. We are extremely grateful for his friendly support and professionalism. We express our heartfelt gratitude to our Head of Department Prof. D. R. Ingale and our project coordinator Prof. B. W. Balkhande for their help and support. This task would not have been possible without the help and guidance of our project guide Prof. Sheetal Thakare. We are also convening special thanks to all staff of Computer Engineering Department for their support and help. Last but not least, we are very much thankful to our friends who directly or indirectly helped us in completion of the project report.

REFERENCES

[1] D. Hong, S. Man, B. Hawes, and M. Mathews. A password scheme strongly resistant to spyware. In *in*

Proceedings of International conference on security and management, Las Vergas, NV, 2002.

[2] J. Thorpe and P. C. v. Oorschot. Towards secure design choices for implementing graphical passwords. In *in Proceedings* of the 20th Annual Computer Security Applications *Conference*, Tucson,Arizona, 2004.

[3] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in Symposium on Usable Privacy and Security (SOUPS). Carnegie-Mellon University, Pittsburgh, 2005.

[4] 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, 1999.

[5] S. Chiasson, "Usable authentication and click-based graphical passwords," Ph.D. dissertation, School of Computer Science, Carleton University, December 2008.

[6] F. Tari, A. Ozok, and S. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," in 2nd ACM Symposium on Usable Privacy and Security (SOUPS),2006.

