Passblot: A Highly Scalable Graphical One Time Password System

Sainath Gupta, Shashank Sahni, Pruthvi Sabbu, Siddhartha Varma,
Suryakanth V Gangashetty

IIIT – Hyderabad, Gachibowli, Hyderabad, India 500032

{sainath.gupta, shashank.sahni, pruthvireddy.sabbu,
siddhartha.varma} @research.iiit.ac.in, svg@iiit.ac.in

ABSTRACT

User authentication is necessary to secure the data and process on Internet and in digital devices. Static text based authentication are most widely employed authentication systems for being inexpensive and highly scalable. But they are prone to various types of active and passive attacks. The constant need of extending them to increase security is making them less usable. One promising alternative is Graphical authentication systems, which if implemented properly are more secure but have their own drawbacks. In this paper, we discuss in detail the extension of our previous work Passblot [18], a unique graphical authentication system. It generates pseudo random one time passwords using a set of inkblots, unique to each user. Properties of one time passwords ensure the resistance towards various common attacks and the uniqueness of human perception makes it usable. We demonstrate how our system effectively mitigates various attacks and analyse the results from various experiments conducted.

KEYWORDS

Usable security, Authentication, one-time passwords, Interfaces, Security, Cueing.

1. INTRODUCTION

An average Internet user has around 25 accounts that require passwords [37]. People tend to forget their passwords [8, 9] due to human memory's fallibility and need reminders or replacements. Cost of replacement is anything but negligible and has to be funded. As well, some users tend to use unsafe practices like writing them down, saving it in email drafts, personal computers, reusing the same password across multiple sites, or frequently reinitializing passwords upon failure to authenticate [10, 11, 12, 13].

To counter ever increasing dictionary attacks, they compel users to increase the attack space of the password. Even though an addition of special character, number, capital alphabets helps in mitigating the dictionary attack, but they are still prone to replay, session hijacking, shoulder surfing and key logger attacks, in addition to being a cognitive burden.

One of the promising alternatives for current authentication systems is the Graphical password scheme. They have advantage of being more secure in terms of writing down and verbal

DOI : 10.5121/ijnsa.2012.4215

disclosure. Many Graphical Authentication systems [1, 2, 4, 24, 25, 26, 27, 28, 29] have been proposed which club usage of graphical and text schemes. However, they are susceptible to several types of active and passive attacks like replay, shoulder surfing, session hijacking and man in the middle attack.

To address the above issues, we proposed a new inkblot based graphical password system known as Passblot [18], which is resistant to most of the attacks mentioned above. Passblot has the following salient features.

i. Immune to replay, dictionary attacks and simple key logger attacks.
ii. Robust against brute-force and blind attacks.
iii. One-time password for every login.
iv. Can be used to overcome man in middle attack and session hijacking.
v. Scalable with the current text based authentication systems.

In this paper, we describe the complete design of our scheme and discuss the potentials attacks on Passblot and how they are mitigated. We conducted two user studies with 35 and 10 participants for the period of eight days. Results show that, users had high success rates and as well participants rated the system positively.

2. RELATED WORK

For a long time, studies have shown the human brain's superior memory for recognizing and recalling visual information as opposed to verbal or textual information. This affect is generally attributed to Picture superiority effect [34] and as well to dual coding effect [19].

Based on cognitive activity required, Graphical authentication systems can be classified into four categories [21]. They are Recognition, Full recall, Cued recall and Cued recognition

In recognition based graphical password system, user memorizes a list of images during registration and must recognize those images among decoy images to login. Some of the well known examples are Passfaces [24], Use your illusion [26] which were initially thought to be secure but were cracked owing to predictable patterns. In the systems proposed by Pering [27], Tulis[28], Renaud [29], user's personal images were used as passwords. These images remain closely related to the person and thus are insecure in a practical scenario.

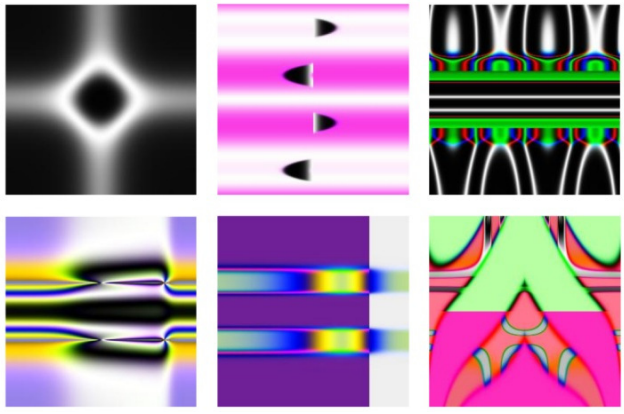

Figure 1. Images used in Dejavu [25], recognition based graphical authentication system.

Pure recall is when a user is required to remember the password without any assistance. It is supposed to be most difficult, since user must remember password without any assistance from the system. Text passwords fall under this category. For graphical passwords, the user is required to either remember or draw an image during registration and repeat it during login. Draw-A-Secret [30], Pass-Go [31] and Pass-Doodles [32] used a set of pre-defined grids for the visual drawing. The drawbacks of these methods were the users' habit of drawing symmetric images with few strokes, thus decreasing the password space. Other's remembered the drawing but couldn't recall the positions precisely. In addition to these, such authentication methods are easily susceptible to shoulder surfing attacks. Pattern lock used on smart phones is one such example.

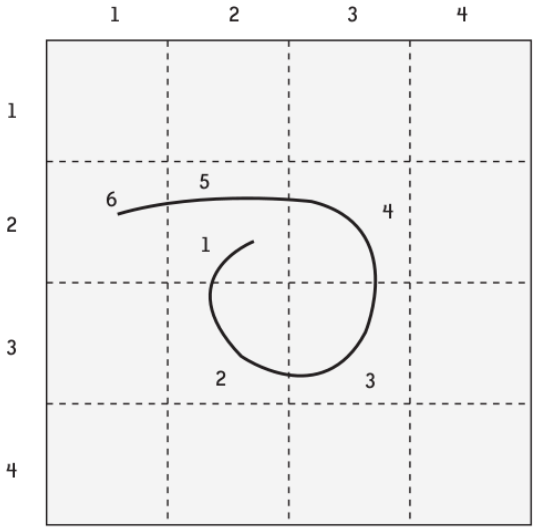

Figure 2. Draw a Secret(DAS) uses a 4x4 grid to let user draw a pattern for authentication

An interesting approach is Cued recognition, where a cue helps the user in the recognition of portfolio images. Some interesting schemes are Story scheme by Davis. [22] and ImageShield[23]. In Story scheme, a story or the semantic relationship between the images assists the user in the recognition of password images. Even though it offers better resilience against guessing attacks when compared to PassFaces[24]), users had problems in remembering their story passwords correctly and often forgot the order. The reason for this was they picked images that looked attractive and tried to remember them even though they were advised to choose stories.

Cued recall authentication scheme, is another interesting mechanism where user is given a cue that aids the recall of password from memory. Best example of cued recall scheme is PassPoints [33] and Cued Click points, where password is constructed with series of random clicks on predefined region of an image. For login, the user is supposed to click the locations in the same order. This method was found vulnerable to dictionary attack as users chose semantically meaningful regions of the image (i.e., hotspots) as click points.

InkBlot authentication is another cued recall based scheme [1]. It uses inkblot like abstract images as cue for text password entry. It is vulnerable to most of the common attacks like shoulder surfing, MITM replay attack etc. Moreover, once the password is compromised, the entire process of registering has to take place again which demands more time**.**

The cueing mechanism should be ideal enough to help users to remember their passwords easily but should provide no clues to any malicious user.

3. OUR PROPOSAL

Authentication in Passblot is based on inkblots' mnemonic similar to the scheme introduced in [1], but has enhanced security. Even though we can generate inkblots on the fly, we chose to use ten inkblot-like random images taken from inkblot authentication system [7] with the required permissions.

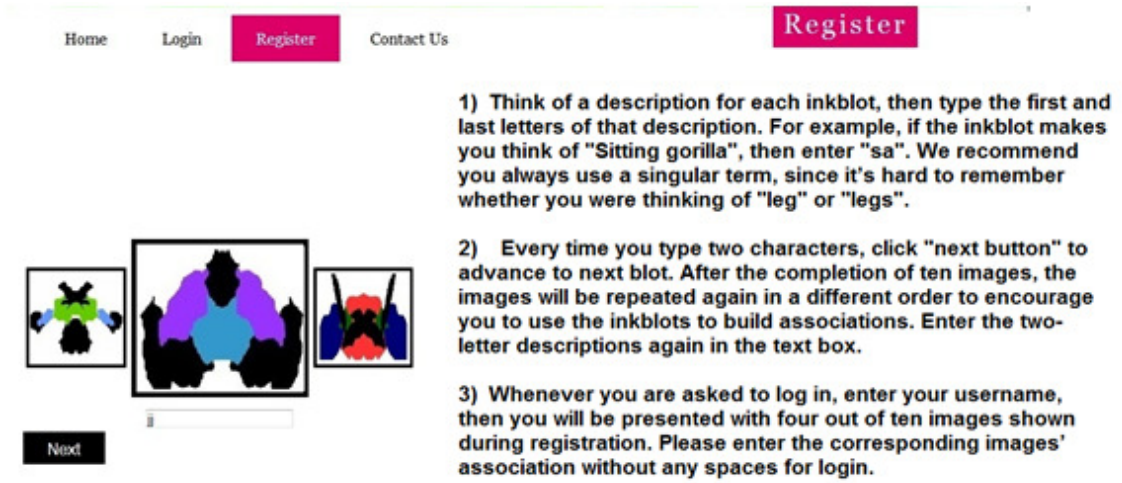

Figure 3. Registration page screenshot of Passblot

During registration, a user registers using their respective email ids as usernames. They were given the selected 10 inkblots one by one as shown in Figure 3 and asked to think of a description for each inkblot. And then type the first and last letters of the description which can be referred as an association to that inkblot or hash of the description. After that, the users were again shown the same inkblots in a different order to confirm the corresponding associations and as well to prevent them from forming their own associations.

In the authentication phase, when the user inputs his user ID, he is shown four out of the ten inkblots that he was shown during the registration phase and is asked to input the corresponding associations. The process is as shown in Figure 4. The Authentication system authenticates the user if atleast three out of four associations are valid.

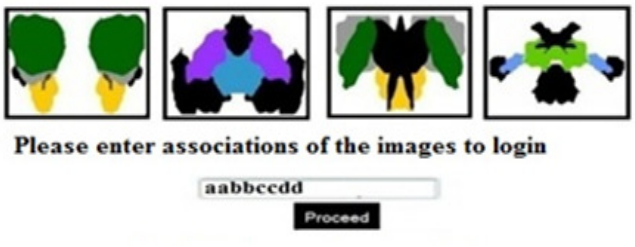

Figure 4. Login of Passblot

For example, let the associations made during the registration phase to the inkblot images Inkblot 1, Inkblot 2, Inkblot 3, Inkblot 4(shown in Figure 4) be aa, bb, cc, dd respectively. Then the password for this particular session will be aabbccdd. To make the system more usable, the user can also be authenticated even if one of the association is wrong, the following associations i.e., xxbbccdd or aaxxccdd or aabbxxdd or aabbccxx are also authorized associations to login to the system.

We have conducted a user study to analyze our system's security, ease of use. The analysis is discussed in the following sections.

3.1 User study I

Our previous user study was conducted on two platforms (i.e., on personal computers and smart phones) conducting three different experiments in total.

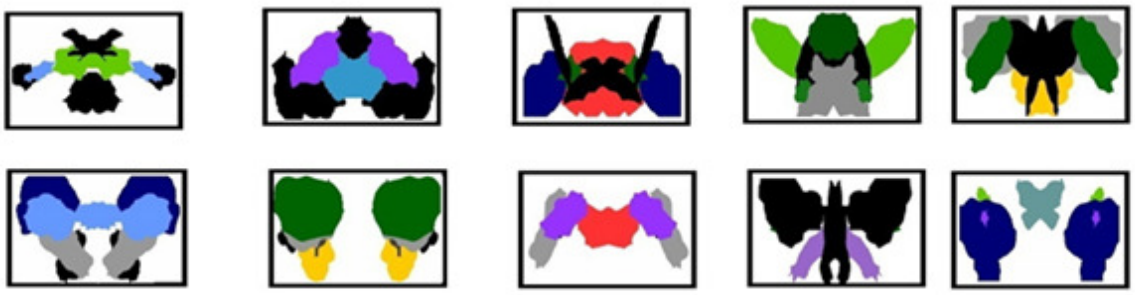

Figure 5. Ten images used for the experiment

i. The first experiment was conducted on 30 volunteers using their Personal Computers in their own work space as we wanted to keep the experiment close to the real-life conditions. Both registration and login phase were conducted as discussed in Section 3.
ii. The second experiment was conducted to analyze the experience on smart phones. This experiment involved five users, using smart phones with Wi-Fi access and QWERTY keypad. In this experiment, users were encouraged to carry out the registration phase on the Personal Computers to avoid the effect of vexation on the process, caused due to

slightly extended time-consuming registration method. And the complete login phase is conducted normally on the smart phones.

iii. The third experiment happened in parallel with the first experiment where six volunteers were asked to use the standard text based password authentications.

A total of 41 undergraduate students and Research Associates volunteered for the prototype testing. 16 of the volunteers are female and rest 25 of them were male, with ages between ranging 18 to 31, there median age being 23.

Users were sent an email with complete instructions and a link to the website. The set of instructions are also shown in the login page as shown in figure 1. Users were also given a demo of the concept before the experiment.

The experimental procedure has the following phases:

1. **Registration**: The users were asked to register using their respective email ids as usernames. They were initially shown 10 inkblots one by one as shown in Figure 1, and asked to enter an association to that inkblot. After that, the users were again shown the same inkblots in a jumbled order to confirm whether they associated properly and as well to prevent them from forming their own associations. There was no time constraint placed on the whole process to analyze the ease with which the user is using the system. After the registration, the users had to login twice to get familiarized with the system (these logins were not used in our analysis).
2. **Authentication**: During login phase, the user is asked to enter his user name. Once the system confirms his username, it shows 4 inkblots randomly chosen out of the 10 inkblots, as shown in Figure 2, that were used in registration phase by that particular user. The user then enters the unique 8 character pass-phrase (concatenation of the 4 inkblots' associations). Login success rate and time taken to complete the process were recorded.

The users were asked to login in as follows:

1. Twice after one hour of registration
2. Once the next day.
3. Once next week

Users could also request a re-registration from the website administrator by email if the password had been forgotten. All accesses were logged to facilitate analysis. Experimental analysis and their results are presented in the section 4.1.

3.2 User study II

In our latest study, we gave a task which required the user to transfer amount from one pseudo bank account to another pseudo bank account which needs authentication to proceed.

In registration phase, images were registered as in user study I, user was also asked to give a strong text password which is of minimum 6 characters, consisted of at least one Capital letter, one numerical, one special character he has to enter it twice for confirmation.

In Authentication phase, for half the study group it was first Passblot authentication then task and then strong text password authentication then repeat the task again and for the rest half of the study group it was strong text password authentication first then task and then Passblot authentication, then repeat the task again. Only three login attempts were allowed for any authentication process.

The users were asked to login in as follows:

1. Registration and training
2. Once the next day
3. Once next week

Users could also request a re-registration from the website administrator by email if the password had been forgotten. All accesses were logged to facilitate analysis. Experimental analysis and their results are presented in the next section. There was no overlap between participants from earlier studies.

4. ANALYSIS AND RESULTS

4.1 In User Study I

Results shown in Table 1 are of User study I, which show us that most of the users where able to login in session 1 and session 2, but for session 3, some users had problem remembering the associations. Since, there was not much difference between Personal computer and mobile users login we clubbed them both. There were a total of 137 successful logins (Mean time (M): 23.737 s, Standard Deviation (SE): 9.438).

Table 1: User Study I Login Success rate

Session	No of successful logins	No of users with first Attempt failed
Session 1	70	1
Session 2	34	3
Session 3	33	6

Another interesting finding that we found was that some of the users associated the inkblots in their native language like French, Hindi and Telugu. This will increase the entropy of the inkblots' associations than their regular 4 bits per character.

4.2 In User study II

Results shown in Table 2 are of User study I, which show us that most of the users where able to login in session 1 and session 2, there were a total of 33 successful logins.

Table 2: User Study II Login Success rate

Authentication type	Session 1 (Day 1)			Session 2 (Day 8)		
	Average Time for login	Number of users with more than one login attempt	Total Successful logins	Average Time for login	Number of users with more than one login attempt	Total Successful logins
Passblot	23.48 s	1	10	24.14 s	2	9
Strong Text Password	9.76 s	3	8	6.85 s	6	6

The results show that Passblot must be considered as a viable substitution for strong text passwords that are being currently implemented. The less time on part of the Strong text passwords made us doubt that users who successfully logged in session 2 might have used passwords which they regularly might be using for other accounts, this was later confirmed during our interaction with them.

Any good authentication mechanisms, must try to maximize both security and ease of use with neither taking the upper hand. The following two sub sections will analyse our results of Passblot assisted authentication in terms of these perspectives. The main aim of these experiments is to determine whether the level of cognitive processing required in using Passblot was acceptable to users. In addition to the quantitative analysis of logging records, we also analysed responses to a questionnaire given to the website users.

5. ANALYSIS

5.1 Security

Our scheme provides much better security against many types of active and passive attacks than many other authentication schemes. We describe some of the general password attacks and resistance of our scheme against them.

5.1.1 Immune to Replay attack and Key loggers

Replay attack involves intercepting a stream of messages between two parties and replaying the stream as is to one or both ends. In this way, if the attacker access to the password sent by the user, attacker can use it to log in as the user.

Since, we are using a separate set of images for each subsequent login, our system requires a unique pass phrase for each session to authenticate. As a result of our one time password scheme even if an intruder intercepts a user's password for once, he won't be able to use it for login, making it immune to replay attacks.

Key-logger is a software program or hardware device that monitors each keystroke user types on a keyboard. Attacks involving key-loggers will not successful against our system, due to the usage of a one-time password for each log in session.

5.1.2 Dictionary attack

Dictionary attacks use a targeted technique of successively trying all the words in an exhaustive list of likely possibilities, usually called as dictionary. Passblot authentication mechanism involves human perception and as of now, there is no known dictionary which lists out such possibilities.

Ideally, such a list shall have numerous associations for every image. Hence, such a creation of one such dictionary would be constrained by the set of images and association's search space. This space could be very high if we don't restrict it to be expressed in 26 English alphabets. More ever, since each user has his own set of unique images, which will make such a dictionary creation very resource intensive.

Clearly, any attempt will be very resource intensive with a meagre chance of success. Hence, dictionary attack cannot be successful.

5.1.3 Brute force and blind attacks

For a successful login, at least 6 characters out of 8 characters have to be correct. Since, there are 26 possibilities for each character in the pass-phrase. Hence the probability for blind or brute force attack to succeed is $1/ (26^6)$.

This is when we assume that all associations to be English alphabets. We can massively increase this space by facilitating Unicode for entering associations. After all, one can't expect everyone to be using an English keyboard. Our study shows that some users associate in their native language. Consider a scenario where a user associates the images in Chinese. The number of most general Chinese characters used in modern times is around 7,000[20]. As a result of this, the probability drops down to $1/(7000^6)$. Similarly, adding multi-lingual support will almost neutralize brute force attack.

Another way to increase the password space would be increasing the number of authentication images.

5.1.4 Resistant to shoulder surfing attack

Shoulder surfing is using direct observation techniques, such as looking over some one's shoulder, to get information. Due to advent of cheap and high resolution cameras it has become

very easy for a malicious user to capture data, which is big threat for both static password system and graphical passwords.

Even though an attacker observes or records one successful authentication pass-phrase, he gets only partial information on the associations. The worst case scenario where 3 consecutive login pages contain all the 10 inkblots is the best chance for the attacker to know all the inkblot's associations. Given, the probability that two consecutive sets of 4 inkblots are the same is 1/10C4, the attacker usually have to be successful for minimum of 3 times which makes it more robust compared to other authentication schemes.

5.1.5 Man in the middle, Interception and Session hijacking attack

Man in the middle (MITM) is the form of attack in which an eavesdropper opens and maintains active connections with both the parties and relays messages between them.

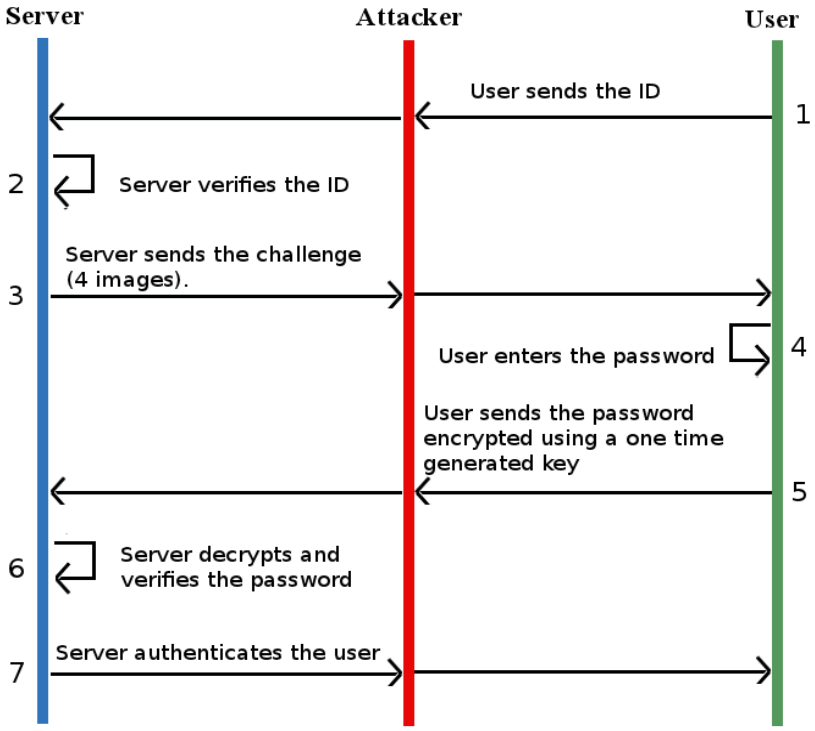

Figure 6. Illustration of Passblot Protocol

Such an attack on the previous implementation of Passblot would yield the password. To be secure against this kind of attack, we have made use of the fact that both the parties know the one time passwords for every session. Since, every login produces a different eight character password, we can use it as a seed to generate an encryption key for encrypting the password before sending it to the server. Since, the server knows the correct password for the session it

will be able to decipher and verify authentication. In this way, the password will never be sent in plain text, making interception useless.

In a similar way, one can use the password to generate a onetime session key for each session, preventing a session hijacking attack.

5.1.6 Social Engineering Attack

In a social engineering attack, someone attempts to obtain your password, while masquerading as a support technician or other authorized personnel who need your authentication credentials, relying on social engineering. The inherent feature of this system's inability to share password data makes this attack infeasible.

5.1.7 Implements a strict policy of using different passwords for different sites

Some cases of data and system compromises were as a result of user's negligence. People tend to keep passwords as simple as possible. They usually go for day to day words leaving them wide open to dictionary attack such as their daughter's or pet's name making the password deductable by any malicious user. To make things worse, sometimes use the same password everywhere like on personal computers, corporate email, administrator's password etc.

Passblot authentication scheme helps implement a strict every account different and unique password policy. For different web based authentications, the systems uses different sets of images for registration which are generated on the fly during registration, resulting in different associations hence different passwords.

This will prevent complete breakdown of a user's online portfolio even though one of his user accounts is compromised.

5.2 Ease of use

In this section we focus on the results and the feedback gathered from our experiment to measure the user's experience while using our system when compared to the traditional password system.

We start at the logical beginning and discuss our registration procedure. Although it is often glossed over, the registration of a system can play a vital role in forming the user's initial perspective of the system. During our experiment, there was no time restraint placed upon registration process. As many users have never used graphical authentication systems before the experiment, we found that many users spent considerable amount of time during the registration phase (Mean time M: 210.257 s, Standard Deviation SE: 80.343 s).

This can be viewed as a positive or negative effect depending on the reader's point of view. It clearly makes the registration less stressful, which is a good thing and is likely to lead to more memorable passwords but increases the registration time.

We continue our discussion by considering the mean length of time (measured in seconds) required to login for successful sessions. This measurement was taken from the moment the user enters his username to the point when the login session is completed.

We found that there was a significant difference between Passblot (M: 23.737 s, SE: 9.438 s) and normal text passwords (M: 12.545 s, SE: 3.363 s). This value includes any additional time it would have taken for the user's browser to download and display the image representing the inkblot. During the course of the experiment there were a total of 137 successful login sessions for Passblot and 22 successful login sessions for static passwords. Also, the users didn't login strictly on time.

The questionnaire revealed that while most users felt that they understood how to use the Passblot, at least some found it hard to describe their inkblots, and to retain their description. But, almost all of them appreciated the enhanced security of the system. There is an implicit understanding that any authentication mechanism teeters between security and usability and a weakening of the one will lead to a strengthening of the other. This is also the case when Passblot was used.

5.2.1 Qualitative evaluation

After the experiment, we had informal discussions with all participants to elicit opinions of the Passblot. We hoped that after using the system on their own personal computers for one week they would have stronger and more interesting comments than if we had performed a short lab study.

Some interesting and recurring comments received were the following:

"I would like to skip few of the inkblots."

"'I would prefer to choose my own inkblots."'

"'During registration, I thought we saw funny images, I showed it to my lab mate(s)."'

Even though we wanted to give an option of skipping, we ruled against it since, more abstract the images more unique the associations. By this the password selection becomes uniform making it difficult for the attacker. Users usually choose alphanumeric passwords and PINs in predictable ways [35], which is also noted in graphical password studies [45].

After the end of User study II, we requested users to answer a simple question

"How do you like Passblot on basis of Usability and security?"

Available responses to this question were based on three options Like, Neutral and dislike.

As one can see from Table 3, Users showed high levels of satisfaction when it comes perception of usability and security.

Table 3: Questionnaire responses which show high levels of

User satisfaction

Response	
Like	6
Neutral	3
Dislike	1

We also asked the ones who have successfully logged in using Strong text password behind the short time taken for authentication, as we thought, we found that four of them reused passwords i.e., used passwords which they use on other online accounts.

The interaction revealed that while most users felt that they understood how to use the Passblot, almost half found it hard to describe their inkblots during registration. But, almost all of them appreciated the enhanced security of the system. There is an implicit understanding that any authentication mechanism teeters between security and usability and a weakening of the one will lead to a strengthening of the other. This is also the case when Passblot was used.

CONCLUSION AND FUTURE WORK

In this paper, we presented and analysed Passblot, a simple, highly scalable and strong authentication system, which is simple enough for users to use and strong enough to keep malicious users away. Its strength lies in its simplicity and unique perception of each individual. This work contributes design and evaluation of a new graphical password authentication system that extends the challenge-response paradigm to resist various active and passive attacks. We designed and tested a prototype of Passblot. Empirical studies of Passblot provide good evidences of Memorability.

One key limitation however, is that login durations recorded for our systems are long. User acceptance is often driven by convenience and login durations of approximately 23 seconds is unattractive to many users. Hence, we feel that this system is best implemented where there is a need of enhanced security like in Bank transactions, corporate communications, in places where network cannot be trusted or additional security is needed.

Our experiment sample comprised of only students and research scholars, but since this was an experimental study, we used a convenient sample. In future, we plan to use a bigger and diverse sample for more accurate results

Acknowledgement

I would like to thank Mr. Jeremy Elson of Microsoft for allowing us to use the images. Mr. Rohit A Khot for being an inspiration for my research.

I would also like to thank Mr. Avinash Jain for his support in conducting the experiment, and also all the volunteers that participated/helped in the user study for spending their time and giving us valuable feedback on the system.

References

1. A. Stubblefield and D. Simon. Inkblot authentication. Technical Report MSR-TR-2004-85, Aug. 2004.
2. Real User Corporation. The science behind Passfaces, 2001. http://www.realusers.com.
3. D. Weinshall. Cognitive authentication schemes safe against spyware. In Proc. IEEE Symp. Sec. and Privacy May 2006.
4. Dhamija, R., Perring, A. (2000). Déjà vu: A User Study Using Images for Authentication. Proceedings of the 9th USENIX Security Symposium.
5. M. Hertzum, Minimal-feedback hints for remembering passwords, Interactions (2006) 38–40.
6. A. Paivio representations: A dual coding approach, Oxford University Press, Oxford, UK, 1986
7. Inkblot Authentication system www.inkblotpassword.com
8. Ensor, B. How Consumers Remember Passwords. Forrester Research Report, June 2, 2004.
9. Florencio, D. and Herley, C. A large-scale study of web password habits. Proceedings of the International Conference on World Wide Web, (WWW 2007), 657-666.
    a. Adams, A. and Sasse, M.A. Users are not the enemy. Communications of the ACM, (CACM Dec 1999), 40-46.
    b. Adams, A., Sasse, M.A., and Lunt, P. Making passwords secure and usable. Proceedings of HCI on People and Computers XII, (HCI 1997), 1-19.
10. BBC News. UN warns on password 'explosion'. http://news.bbc.co.uk/2/hi/technology/6199372.stm.
11. Gaw, S. and Felten, E. Password management strategies for online accounts. Proceedings of the Symposium on Usable Privacy and Security, (SOUPS 2006), 44-55.
12. Ives, B., Walsh K.R., and Schneider, H. The domino effect of password reuse. In Communications of the ACM, (CACM Apr 2004), 75-78.
13. Morris, R. and Thompson, K. Password security: A case history. Communications of the ACM (CACM Nov 1979), 594-497.
14. R J. Witty and K Brittain. Automated password reset can cut IT service desk costs, 2004. Gartner Report.
15. M. Paik, “Stragglers of the Herd Get Eaten: Security Concerns for GSM Mobile Banking Applications,” HotMobile 2010: The Eleventh International Workshop on Mobile Computing Systems and Applications, Maryland: ACM, 2010.
16. Karen Renaud, “Password Cueing with Cue (ink) blots”, www.mcbryan.co.uk/papers/cueblots.pdf

17. Ayannuga Olanrewaju O, Folorunso Olusegun, Akinwale Adio, "Evalution of a usable hybrid authentication system" International Journal of Computer Applications (0975 – 8887) Volume 17– No.8, March 2011.

18. Sainath Gupta, Pruthvi Sabbu, Siddhartha Varma and Suryakanth V.Gangashetty. "Passblot: A Usable Way of Authentication Scheme to Generate One Time Passwords." CNSA 2011, CCIS 196, pp. 374–382, 2011. © Springer-Verlag Berlin Heidelberg

19. Chiasson S., Forget A., Stobert E., van Oorschot P., and Biddle R. September 2008. Multiple password interference in text and click-based graphical passwords. (Manuscript under submission). Technical Report TR- 08-20, School of Computer Science, Carleton University.

20. Multiple Authors, "List of generally used characters in modern Chinese". Wikipedia http://en.wikipedia.org/wiki/Chinese_character

21. Cranor, L., and Garfinkel, S. Security and Usability: Designing Systems that People can use. O'reilly Media,2005.

22. Davis, D., Monrose, F., and Reiter, M. K. On user choice in graphical password schemes. In Proc. 13th USENIX Security Symposium (2004).

23. ImageShield™ http://www.confidenttechnologies.com/products/confident-imageshield

24. Brostoff, S., and Sasse, M.A. Are Passfaces more usable than passwords? A field trial investigation. Proceedings of HCI on people and Computers XIV,(HCI 2000), 405-424., Pass09

25. Dhamija, R., and Perrig, A. 2000. Deja Vu: a user study using images for authentication. In Proceedings of the 9th Conference on USENIX Security Symposium - Volume 9 (2000). 4-4

26. Hayashi, E., Dhamija, R., Christin, N., and Perrig, A. 2008. Use Your Illusion: secure authentication usable anywhere. In Proceedings of the 4th Symposium on Usable Privacy and Security (2008). SOUPS '08, 35-45.

27. Pering, T., Sundar, M., Light, J., and Want, R. 2003. Photographic Authentication through Untrusted Terminals. IEEE Pervasive Computing 2, 1 (Jan. 2003), 30-36.

28. Tullis, T. S., and Tedesco, D. P. 2005. Using personal photos as pictorial passwords. In CHI '05 Extended Abstracts on Human Factors in Computing Systems (2005). CHI '05. ACM, 1841-1844.

29. Renaud, K. 2009. On user involvement in production of images used in visual authentication. J. Vis. Lang. Comput. 20, 1 (Feb. 2009), 1-15.

30. Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., and Rubin, A. D. 1999. The design and analysis of graphical passwords. In Proceedings of the 8th Conference on USENIX Security Symposium. 8(1999). 1-1.

31. Tao, H., and Adams, C. Pass-go: A proposal to improve the usability of graphical passwords. Int'l Journal of Network Security. 7(2008), 272-292

32. Goldberg, J., Hagman, J., and Sazawal, V. Doodling our way to better authentication (student poster). In ACM Conference on Human Factors in Computing Systems (CHI), April 2002.

33. Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., and Memon, N. 2005. PassPoints: design and longitudinal evaluation of a graphical password system.Int. J. Hum.-Comput. Stud. 63, 1-2 (Jul. 2005), 102-127.

34. Nelson, D.L., Reed, U.S., and Walling, J.R. Picture Superiority Effect. Journal of Experimental Psychology: Human Learning and Memory 3, pp. 485-497, 1977.

35. KLEIN, D. Foiling the cracker: A survey of, and improvements to, password security. Proceedings of the Second USENIX Security Workshop (Aug 1990)

36. Thorpe, J., and van Oorschot, P. C. 2007. Human-seeded attacks and exploiting hot-spots in graphical passwords. In Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium (2007).1-16.

37. Florencio, D., and Herley, C. A large-scale study of web password habits. In Proc. WWW 2007, ACM Press (2007), 657-666.