Divide and Conquer Approach for Solving Security and Usability Conflict in User Authentication

Shah Zaman Nizamani
Department of IT
Quaid-e-Awam University
Nawabshah, Pakistan

Waqas Ali Sahito
Department of IT
Quaid-e-Awam University
Nawabshah, Pakistan

Shafique Awan
Department of Computer Science
Benazir Bhuto Shaheed University
Liyari, Pakistan

Abstract—**Knowledge based authentication schemes are divided into textual password schemes and graphical password schemes. Textual password schemes are easy to use but have well known security issues, such as weak against online security attacks. Graphical password schemes are generally weak against shoulder surfing attacks. Usability is another issue with most of the graphical password schemes. For improving security of knowledge-based authentication schemes complex password entry procedures are used, which improve security but weakens useability of the authentication schemes. In order to resolve this security and usability conflict, a user authentication scheme is proposed, which contains one registration and two login screens called easy and secure login screens. Easy login screen provides easy and quick way of authentication while secure login screen is resilient to different online security attacks. A user has to decide based upon the authentication environment, which login screen to be used for authentication. For secure environment, where chances of security attacks are less easy login screen is recommended. For insecure environments where chances of security attacks are high, secure login screen is recommended for authentication. In the proposed scheme, image based passwords can also be set along with alphanumeric passwords. Results suggest that proposed scheme improves security against offline and online attacks.**

Keywords*—*Authentication; alphanumeric passwords; security; passwords memorability

I. Introduction

Textual password scheme is easy to use because it has very simple password entry procedure. However, this scheme is weak in security because passwords can be recorded or observed from the login screen. Textual passwords can also be guessed through dictionary attacks because users mostly use dictionary words in their passwords [1]. In many applications some restrictions are enforced to set strong passwords such as minimum length of passwords. These restrictions does not fully resolve the issue of weak textual passwords because users still use dictionary words after applying the restrictions [2]. Complex or strong alphanumeric passwords are difficult to remember [3], therefore such passwords are not widely used. Strong textual passwords are difficult to guess from offline guessability attacks but they can be theft by observability and recordability attacks [4]. Another issue with textual passwords is that users generally set similar passwords in different accounts [5]. Due to this approach strong alphanumeric passwords can be guessed through offline guessability attacks after hacking a password from one user account [6].

Graphical passwords are used to solve security and memorability issues of textual passwords, but this technique has their own set of problems, specially shoulder surfing and useability related issues [7]. Usability wise an authentication scheme is required to be easy to use, easy to learn and users' satisfaction need to be high with respect to performance and design. While, with respect to security an authentication scheme needs to provide enough resilience against different security attacks. Graphical password schemes lie in the range from secure and less useable to highly usable and less secure. It is because of conflicting nature between security and usability in user authentication schemes.

Different researchers improve the security of graphical password schemes by adding some logic in password entry techniques such as persuasive technique [8]. However, different usability or memorability issues arise due to inclusion of such logic because users have to complete multiple authentication steps or they need to provide large amount of information for authentication.

Security and usability parameters does not efficiently fit into one solution due to their conflicting nature [9]. Therefore, in user authentication schemes either security or usability sacrifices. Researchers generally give more importance to security because it is the most essential feature for an authentication scheme. In this research, both parameters are balanced by two login screens. First screen provides quick and easy way of password entry but it has some security weaknesses against online security attacks. While, other screen is resilient to online security attacks but it requires comparably more time for password entry. Users have option to authenticate with any of the login screen by using same password.

II. Related Work

Passwords in knowledge based authentication schemes are alphanumerical or graphical. Alphanumerical or textual passwords are widely used for authentication but it has security and memorability issues. In order to overcome the issues of textual passwords, graphical passwords are proposed. Graphical password schemes are divided into pure recall based, cued recall based and recognition based schemes [10]. All the categories of graphical password schemes are discussed here in detail.

1) Pure recall based schemes: In this category of graphical password schemes, the passwords consist of some lines. Jermyn *et al.* [11] proposed a pure recall based graphical password scheme known as DAS (Draw-A-Secret). In this scheme, users draw some lines inside 2D grid-based login screen and the lines are considered to be the passwords of the users. In this category, passwords can be quickly inserted but this category of authentication schemes has some security issues. For example, passwords can be easily viewed from login screen and dictionary attacks can also be applied.

Dunphy and Yan [12] proposed modified version of DAS scheme known as BDAS (Background DAS). In this scheme, background image is used inside 2D grid-based login screen. Background image helps the users to set complex passwords [13]. BDAS scheme is weak against shoulder surfing attack because passwords can be easily viewed from the login screen. Android unlock scheme [14] is widely used pure recall based graphical password scheme. In this scheme, nine points are shown in the login screen and the users have to create a password by connecting the points. In Android unlock scheme passwords are easy to enter but this scheme is weak against shoulder surfing attack.

2) Cued recall based schemes: In cued recall based graphical password schemes, passwords consist of some points inside a login screen. Blonder [15] proposed first cued recall based graphical password scheme in 1996. In this scheme, a password is created by selecting some predefined locations inside a picture. For authentication, a user needs to click on the locations which were selected as a password at the time of account registration. Password points are easy to select in Blonder's scheme but it has some security issues such as low password space and weak against shoulder surfing and guessability attack.

Wiedenbeck *et al.* [16] uses the idea of Blonder's scheme and proposed an authentication scheme known as Passpoint. In this scheme, users have no restriction of selecting password points inside the predefined locations. For authentication, a user just needs to click on the points which were selected at the time of password registration. This scheme requires short amount of time for authentication [13] but it is weak against against shoulder surfing attack and guessability attacks [17].

3) Recognition based scheme: Images are used as password elements in recognition based schemes. For authentication, users have to correctly select their password images. Dhamija *et al.* [18] proposed a recognition based graphical password scheme known as Deja Vu, in which Abstract art images are used for password selection. A password is entered by clicking on the password images. Advantage of abstract art images is that they are difficult to guess by the attackers but such images are difficult to memorize. This scheme is also weak against shoulder surfing attacks [13].

CHC [19] is another recognition based graphical password scheme in which large number of icons are shown to the users for password selection. Users are authenticated when they correctly click on the logical triangles formed by the password icons. This scheme is resilient to many security attacks such as shoulder surfing and spyware attacks but it requires large amount of time for authentication. Therefore, usability is the main issue of CHC scheme.

Davis *et al.* [20] proposed another recognition based graphical password scheme known as story scheme. In this scheme, images of different categories are used for password selection. Idea of this scheme is that, users may create stories from password images and the stories will help in memorization of password images. This scheme has password memorability advantage over CHC scheme [19] but this scheme is weak against shoulder surfing attack.

III. Towards Solution

Large number of knowledge based authentication schemes are proposed but easy to use authentication schemes are widely used such as traditional textual password scheme and Android unlock scheme. Relatively secure but difficult to use authentication schemes are not used. For example CHC scheme [19] provides a secure mechanism for authentication but it is not used for authentication due to difficult mechanism of password insertion.

Security and usability have conflicting nature in the field of user authentication, as a result one solution is difficult to design which equally resolves both the conflicting requirements of the authentication process. Therefore, in the proposed scheme users have been provided two options for authentication, one is secure and other is easy to use. Depending upon the login environment, the users can authenticate by any of the login options. Chances of password hacking increases when a user authenticates inside an office or public network, in such environments secure login approach is recommended. While, easy login approach is recommended for private networks such as home. When a user mistakenly authenticate through easy login approach in the insecure environment then same level of password security is achieved which is present in traditional textual password scheme.

IV. Proposed Scheme

In the proposed scheme, one registration and two login screens are designed as shown in Fig. 1. Multiple login screens are designed to solve security and usability conflict in user authentication. In the first login screen (called easy login screen) users just need to type the password elements similar to textual password scheme. This login screen provides easy to use password entry procedure for better usability. Second login screen (called secure login screen) is designed for better security. In the secure login screen, 50% elements (alphanumeric characters and images) are presented. For password entry, users need to enter the count of visible password elements inside the password field. This login screen is resilient to many online security attacks such as keylogger attacks. This login screen provides security advantages but it requires relatively more time for password entry than easy login screen. Therefore, easy login screen is recommended for authentication in secure login environments and the secure login screen is recommended for insecure login environments.

The proposed scheme contains both textual and graphical elements for password selection. A password may be consist of alphanumeric characters, images or combination of both. Users need to remember single password for both the login screens.

A. Registration Activity

In the registration activity, a user inserts profile and authentication information for account creation. Registration screen of the proposed scheme presents twenty four images for password selection as shown in Fig. 2. All the images are selected from the categories of fruits, electronics, birds,

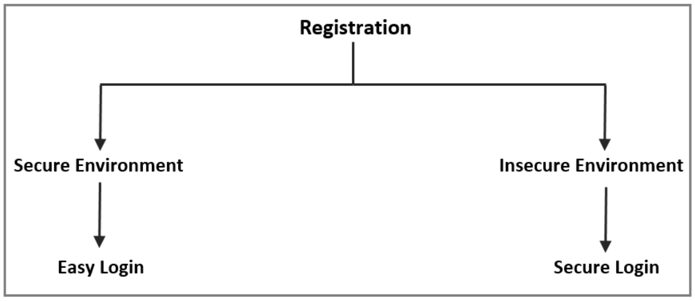

Fig. 1. Proposed solution.

emoji and animals. Four images are selected from each of the category, based upon familiarity among the users.

1) Password entry: Alphanumeric characters of a password are selected by typing the keys of the characters and a password image is selected by typing the shortcut key, which is the combination of “control” and “alter” keys along with two initial characters of an image. For example, if password is “abc” and image of “horse”, then the password is selected by typing “abc” and pressing “ctrl+alt+ho” keys altogether inside the password field. In the database, some Unicode symbols are saved against the password images. For example, in current scenario the image of horse may be represented in the database by Unicode symbol β. The Unicode symbols for the images are not fixed they can be changed in every deployment of the scheme. For improving security against dictionary attacks, it is better to use different Unicode symbols in each deployment of the proposed scheme.

B. Login Activity

In the proposed scheme, login activity can be completed by any of the two login screens. First screen is called “easy login screen” and second is called “secure login screen”. Password entry process is different in both the login screens, which is explained here.

1) Easy login screen: This login screen is almost similar to registration screen as shown in Fig. 3, only fields for inserting profile information are not presented. Password is entered in the easy login screen, similar to the registration screen. A user can insert alphanumeric characters by pressing the keys related with the alphanumeric characters and the images are selected by typing the shortcut keys of the images. After inserting username and password, a user just needs to click on login button for authentication. The user will be authenticated once username and password matches with the stored authentication information.

Easy login screen is designed for quick and easy authentication. Login process of easy login screen is similar to textual password scheme, therefore learnability is not an issue with this login screen. However, security attacks such as keylogger and spyware attacks may work in the easy login screen due to exact insertion of password elements inside the password field. These security weaknesses are intentional because this login screen is designed for better usability. Easy login screen has same security issues as in textual password scheme against online security attacks as same password entry procedure is used. However, this login screen is better in offline guessability attacks because image based passwords can also be selected.

2) Secure login screen: This login screen is designed to resist online secure attacks. All of the attacks are resisted by indirectly gathering passwords from the users. In the secure login screen randomly 50% elements are presented. For authentication a temporary number is inserted into the password field and the number depends upon the visibility of the elements in the secure login screen. The password number changes in every login session, therefore this login screen resist online security attacks.

a) Password entry: In the secure login screen as shown in Fig. 4 and 5, randomly 59 out of 118 (50%) elements are presented. The 59 elements (47 alphanumeric characters and 12 images) are randomly selected but they are shown in natural order. A user has to count the password elements currently visible inside the secure login screen. The count of visible password elements is then inserted into the password field for authentication. For example, if password of a user is “abcde” and an image of “horse” then based upon the login screens as shown in Fig. 4 and 5, the user has to insert “4” in the password field because character “a” and the image of “horse” is not visible in the login screen. If a password contains same element multiple times then the element will be counted more than once. For example, if the password is “abccde” and login screen is same as shown in Fig. 4, then the user has to enter decimal number “5” inside the password field because the character “c” is presented two times within the password.

Login process in secure login screen consists of three steps. In each step different arrangements of alphanumeric characters and images are shown. A user has to count and enter visible password elements for all the three steps. Each step appears by clicking on the tab “Step” as shown at the top of Fig. 4 and 5. Multiple steps are created for reducing the chances of blind guessing attack. The login steps can be increased for improving security against blind guessing attack but it will require more time for authentication.

b) Password matching: In secure login, password numbers are compared for authentication instead of actual password elements. The server generates a password number which is compared with the user’s provided password number. When both the numbers become equal then the server allows sign-in. Steps for authentication in secure login are listed below.

(i) Username and a password number are received by an authentication server.
(ii) If username does not present in the database then the server will close authentication process.
(iii) If username present in the database then the server fetches and decrypt the password based upon the provided username.
(iv) Server gets the session variable which stores all the visible elements for the current login session.
(v) Server counts all the decrypted password elements inside the session variable.
(vi) Server compares the count generated in step V with the password number given by the user.
(vii) A user is authenticated when both the user’s provided number and the system generated count is equal in all the three steps.

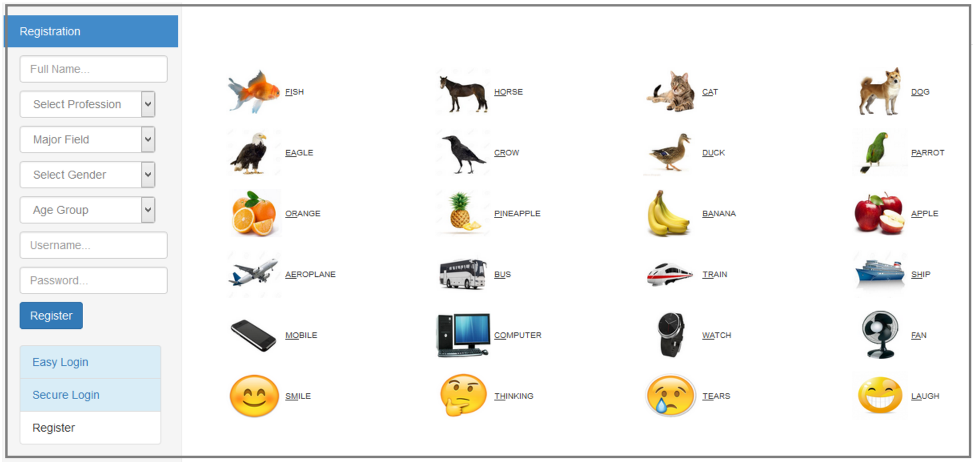

Fig. 2. Registration screen.

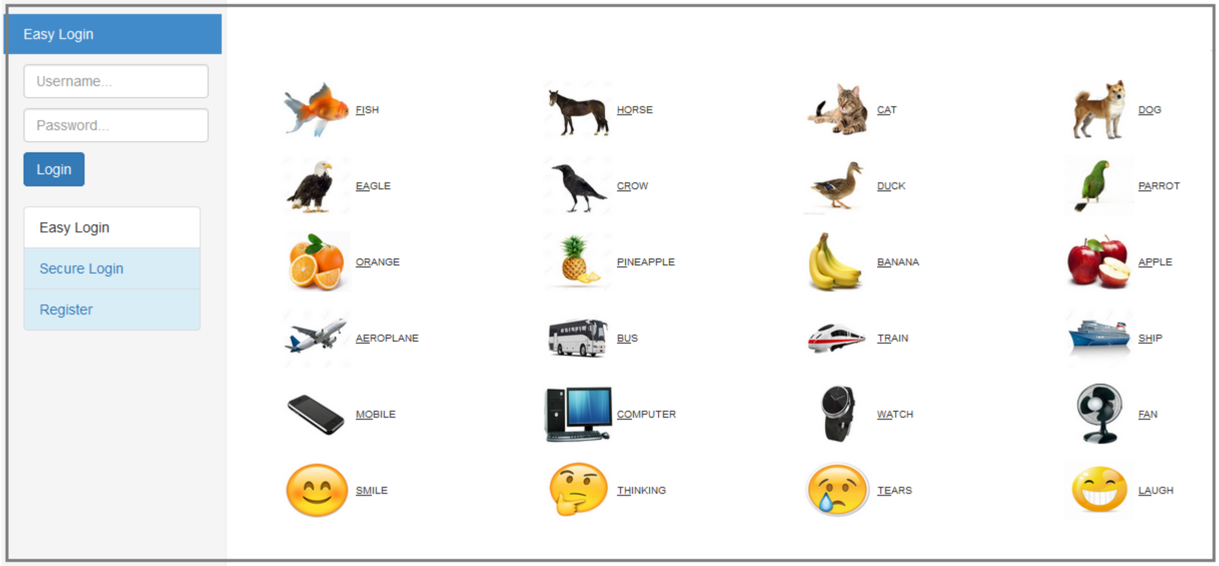

Fig. 3. Easy login screen.

Due to indirect insertion of passwords, the secure login process requires the passwords to be stored in two way encryption. Two way encryption is relatively weak than hashing or one way encryption. Therefore, passwords for the proposed scheme need to be secured with different techniques such as differential masking [21].

V. Usability and Memorability Analysis

In order to analyze usability and memorability aspects of the proposed scheme, a web based application was developed. A hidden process was created inside the application for calculating timings of registration and login activities. A log was also maintained for analyzing failed and successful login attempts.

For testing purpose, 50 participants were selected from different departments of Quaid-E-Awam university of Engineering Science and technology, Pakistan. Professionally the participants were students, teachers and administrative staff. The users were selected based upon their knowledge about computer usage. All the users had basic knowledge about internet and its working. All the participants performed the registration and login activities inside the testing application.

A. Testing Procedure

Testing phase for the proposed scheme was consist of four sessions. In first session, users performed registration and login activities. While in remaining three sessions, users only performed login activities. Before conducting the tests, a demonstration was given for creating user account and sign-in through the testing application. When users fully understood the login and registration activities, then the users were asked to perform the activities inside the application.

Users were free to create any password (alphanumeric or image-based). Minimum length of passwords were set to eight elements and users were also asked to set passwords from at least two categories such as numbers and special characters. Second session was started after one day of registration, in this session the users only performed login activities with their

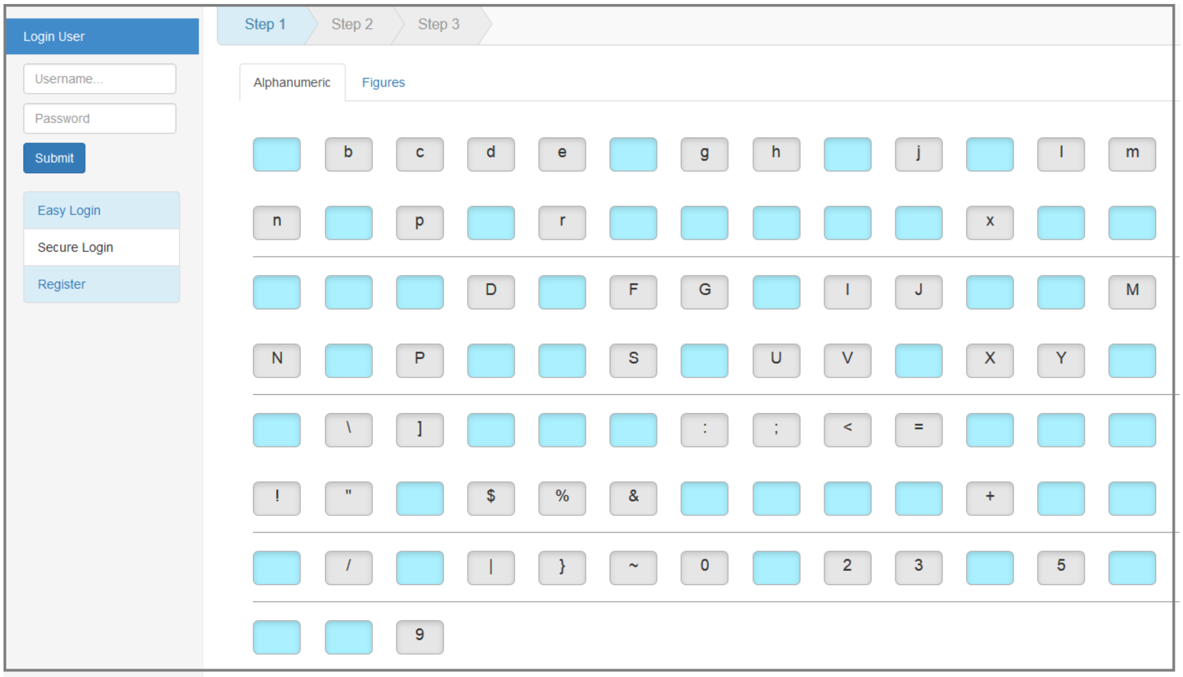

Fig. 4. Secure login screen showing alphanumeric characters.

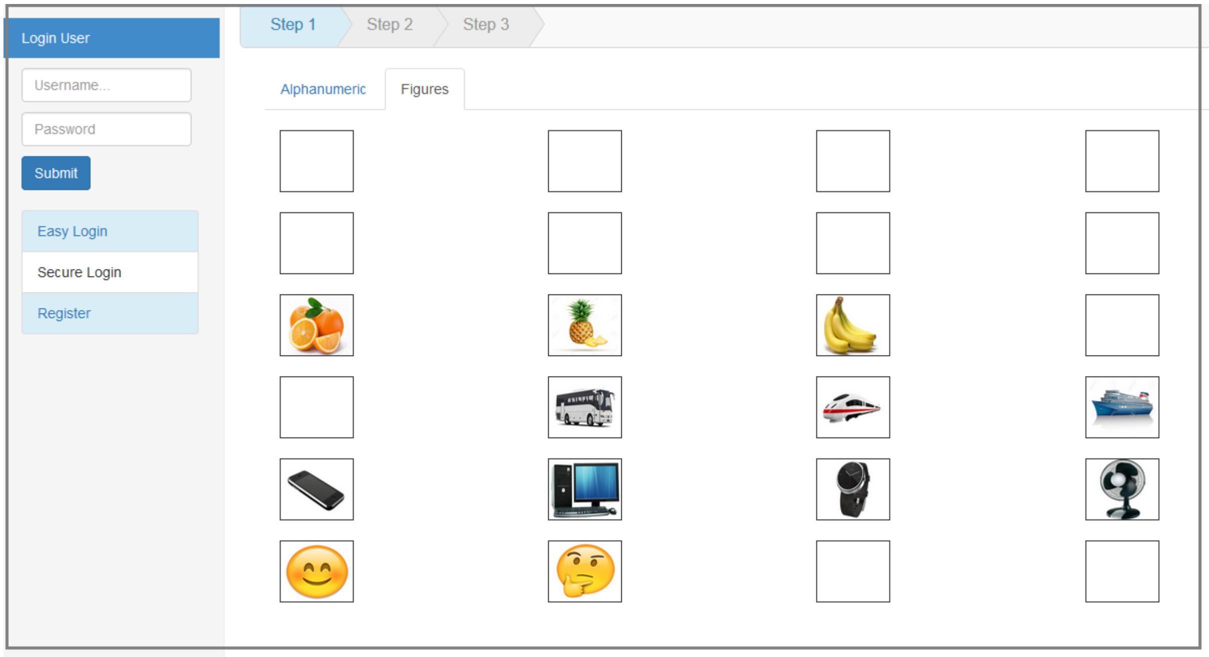

Fig. 5. Secure login screen showing images.

registered username and passwords. Third and fourth sessions were started after one and two weeks of registration, respectively. In both the sessions only those users were asked to login who have successfully authenticated in previous sessions.

B. Testing Results

The experiment data was analyzed to get the performance of the proposed scheme with respect to usability and memorability. Results show that passwords were mostly consist of alphanumeric characters. Out of 50 participants, thirteen users used combination of alphanumeric and image based passwords and three users selected passwords with only images. This behaviour was due to wide use of traditional textual passwords among the users.

Mostly users authenticated in first login attempt when they have remembered their passwords. The results of failed login attempts show that users had no difficulty in authentication inside the proposed scheme.

Authentication timing is the main factor for analyzing usability of an authentication scheme. Testing results showed that the proposed scheme requires 15.82 seconds for password registration or selecting the password elements. Average login time was 11.86 seconds in easy login screen and 32.73 seconds in secure login screen. Large time requires in secure login screen due to three steps of authentication.

The users who used only alphanumeric characters in their passwords took less time in easy login screen in comparison with the users who used images in their passwords. Image based passwords require more time for password insertion due to usage of shortcut keys. The users who set alphanumeric passwords took more time in secure login screen as compared to image based passwords. This behaviour is due to the more effort requires for searching the alphanumeric characters in secure login screen. Average length of the passwords were found 8.9 and average password entropy was found 55 bits.

Memorability tests were conducted immediately after registration, one day, one week and two weeks. The results are shown in Table I.

TABLE I. PASSWORD MEMORABILITY IN THE SCHEME

Duration	Password memorability
After registration	94%
After 1 Day	86%
After 1 Week	72%
After 2 Weeks	62%

VI. SECURITY ANALYSIS

Table II shows the status of different security attacks against textual password scheme, Android unlock scheme and proposed authentication scheme. In Table II value "Y" shows that the login screen is resilient to the particular attack, while the value N shows that the screen is not resilient to the attack. In the table value "Hard" shows that a very high level of effort is required to crack the password.

In the proposed scheme, 118 elements (alphanumeric characters and images) are used, while only 95 elements are used in traditional textual passwords scheme based upon American standard keyboard. Therefore, the proposed scheme provides more password space than textual password scheme. Higher password space is better for security against brute force attack because an attacker needs to apply large number of combinations for password crack.

The proposed scheme also performs better with respect to dictionary attacks because users have option to select images along with alphanumeric characters. Due to the inclusion of images, password dictionaries are difficult to create for the proposed scheme. The attackers have to create the list of passwords with the combination of alphanumeric characters and images and they have to identify the Unicode symbols used for the images.

Shoulder surfing and spyware attacks can be applied in the easy login screen but these attacks are resisted in secure login screen. Passwords are indirectly inserted into the secure login screen, therefore the passwords can not be captured by applying shoulder surfing or spyware attacks in the secure login screen.

Man in the Middle attack depends upon the implementation of the proposed scheme, this attack can be resisted if secure communication channel is used for easy login screen such as SSL or TLS [22] [23]. While, secure login screen is resilient to this attack because users enter temporary numbers instead of actual passwords in the secure login screen.

In multiple recording attack, passwords are captured by recording information of multiple login sessions. In easy login screen, recording of single login session is enough for password heck because a user enters original password elements into the password field. In the secure login screen, different numbers are entered into the password field instead of exact password elements, therefore passwords can not be captured from multiple recording attack.

In blind guessing attack, an attacker randomly enters different passwords into the password field for authentication. In easy login screen this attack does not work because an attacker needs to apply very large number of passwords for authentication, which is not manually possible. In secure login screen, it is possible that an attacker enters three numbers which are the password for current login session. Chances of this threat can be reduced by deactivating the authentication process after three failed login attempts.

Table II shows that easy login screen is weak with respect to client side security attacks but it improves security against offline guessability attacks. While, secure login screen is resilient to most of the security attacks.

VII. CONCLUSION

The proposed scheme does not replaces the traditional textual password scheme but it enhances the security of textual password scheme in terms of password entry procedure and list of password elements. Therefore, proposed scheme can be easily deployed in existing applications which use the textual password scheme for authentication.

Blind guessing attack may work in the secure login screen. Chances of this attack can be reduced by increasing steps inside the secure login screen and adding policies such as allowing only three attempts for authentication.

TABLE II. STATUS OF SECURITY ATTACKS

Scheme	Brute Force	Dictionary	Shoulder Surfing	Spyware	Man in the Middle	Multiple Recording	Blind Guessing
Textual Password	Hard	N	Medium	N	N	N	Y
Android Unlock	N	N	N	N	N	N	Y
Easy login Screen	Y	Y	Medium	N	N	N	Y
Secure Login Screen	Y	Y	Y	Y	Y	N	Hard

In the proposed scheme, number of images can be increased to enhance the password space of the scheme. However, increment should be such that it should not affect the usability or memorability of the scheme. Large number of images can create messy look and feel of the authentication screens and users will face difficulty in finding their password images. Memorability may also be effected by adding or replacing the images with complex images, i.e. the images with less cues for password memorization.

REFERENCES

[1] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password memorability and security: Empirical results," *IEEE Security & privacy*, vol. 2, no. 5, pp. 25–31, 2004.

[2] L. Tam, M. Glassman, and M. Vandenwauver, "The psychology of password management: a tradeoff between security and convenience," *Behaviour & Information Technology*, vol. 29, no. 3, pp. 233–244, 2010.

[3] L. F. Cranor and S. Garfinkel, *Security and usability: designing secure systems that people can use*. " O'Reilly Media, Inc.", 2005.

[4] R. English and R. Poet, "Towards a metric for recognition-based graphical password security," in *Network and System Security (NSS), 2011 5th International Conference on*. IEEE, 2011, pp. 239–243.

[5] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The tangled web of password reuse." in *NDSS*, vol. 14, 2014, pp. 23–26.

[6] A. S. Brown, E. Bracken, S. Zoccoli, and K. Douglas, "Generating and remembering passwords," *Applied Cognitive Psychology*, vol. 18, no. 6, pp. 641–651, 2004.

[7] A. M. Eljetlawi and N. Ithnin, "Graphical password: Comprehensive study of the usability features of the recognition base graphical password methods," in *Convergence and Hybrid Information Technology, 2008. ICCIT'08. Third International Conference on*, vol. 2. IEEE, 2008, pp. 1137–1143.

[8] A. Forget, S. Chiasson, P. C. van Oorschot, and R. Biddle, "Persuasion for stronger passwords: Motivation and pilot study," in *International Conference on Persuasive Technology*. Springer, 2008, pp. 140–150.

[9] Y. Meng, "Designing click-draw based graphical password scheme for better authentication," in *Networking, Architecture and Storage (NAS), 2012 IEEE 7th International Conference on*. IEEE, 2012, pp. 39–48.

[10] 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-Computer Studies*, vol. 63, no. 1, pp. 128–152, 2005.

[11] I. Jermyn, A. J. Mayer, F. Monrose, M. K. Reiter, A. D. Rubin *et al.*, "The design and analysis of graphical passwords." in *Usenix Security*, 1999.

[12] P. Dunphy and J. Yan, "Do background images improve draw a secret graphical passwords?" in *Proceedings of the 14th ACM conference on Computer and communications security*. ACM, 2007, pp. 36–47.

[13] R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Computing Surveys (CSUR)*, vol. 44, no. 4, p. 19, 2012.

[14] S. Uellenbeck, M. Drmuth, C. Wolf, and T. Holz, "Quantifying the security of graphical passwords: the case of android unlock patterns," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 161–172.

[15] G. E. Blonder, "Graphical password," Sep. 24 1996, uS Patent 5,559,961.

[16] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human-Computer Studies*, vol. 63, no. 1, pp. 102–127, 2005.

[17] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "User interface design affects security: Patterns in click-based graphical passwords," *International Journal of Information Security*, vol. 8, no. 6, pp. 387–398, 2009.

[18] R. Dhamija and A. Perrig, "Deja vu-a user study: Using images for authentication." in *USENIX Security Symposium*, vol. 9, 2000, pp. 4–4.

[19] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *Proceedings of the working conference on Advanced visual interfaces*. ACM, 2006, pp. 177–184.

[20] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes." in *USENIX Security Symposium*, vol. 13, 2004, pp. 11–11.

[21] S. Z. Nizamani, S. R. Hassan, and R. Naz, "A theoretical framework for password security against offline guessability attacks," *Indian Journal of Science and Technology*, vol. 10, no. 33, 2017.

[22] A. Freier, P. Karlton, and P. Kocher, "The secure sockets layer (ssl) protocol version 3.0," 2011.

[23] T. Dierks, "The transport layer security (tls) protocol version 1.2," 2008.