Managing the Trade-off Between Usability and Security in Knowledge-Based Authentication

Raghad Alabdullatif, Tahani Alsubait
s43780117@st.uqu.edu.sa, tmsubait@uqu.edu.sa
College of Computer and Information Systems, Umm Al-Qura University, P.O.Box: 715, Makkah, Saudi Arabia

Abstract
Knowledge-based authentication (KBA) is the process where users authenticate their identities by having knowledge of a specific secret which confirms the authentication e.g. passwords. Humans have issues with remembering non-meaningful strings, so they keep choosing weak passwords. This clearly shows the trade-off between usability and security where a decrease in usability might negatively impact security. To overcome this issue, user authentication approaches should find a way to reduce the burden on user's memory so they can choose stronger passwords. The relation between security and usability is much complicated than that. For example, increasing security measures might decrease usability. So, in this paper we argue that this trade-off must be managed effectively. A hybrid authentication system is proposed as an alternative to the traditional password-based authentication. A user study was used to investigate the feasibility of this alternative system by integrating it into a students' university portal.

Key words:
Security, Usability, Knowledge-based authentication, User study

1. Introduction

User authentication is one of the centric components of secure systems to protect them against security threats [1]. The process of authentication is needed to prove that a user has the right to access the system. There is an interesting relation between security and usability aspects of authentication. For example, existing studies have acknowledged that improvements in usability can benefit the security of the system [2].

Moreover, several studies have acknowledged that humans have issues with remembering non-meaningful strings or lengthy alphanumeric passwords. For that reason, users keep ignoring basic security recommendations and practice wrong habits which negatively impact system security. These bad practices include choosing a weak predictable password, using a single password for various applications, or writing down their passwords for easy reference [3][4][5][6][7][8]. Without doubt, the strict policies of choosing passwords have decreased the usability of alphanumeric passwords [9][10]. Increasing the length space of passwords and their randomness will increase the burden on the user's memory, thus, affects the memorability of the password.

More security issues of password-based mechanisms include vulnerability to capture attacks and guess attacks since users tend to create passwords which are memorable and far away from being random. Several studies performed over the last 30 years have shown how easy passwords can be compromised. In 1990, out of 14000 passwords, Klein showed that he was able to crack 25% of them through the usage of a dictionary composed of just 86000 words [11]. An article in Computerworld mentioned that a large company has ran a network password cracker for the purpose of testing it, they successfully cracked about 80% of the passwords in 30 seconds [12]. Reliance on cryptography alone is not sufficient to ensure the security of authentication mechanisms. Given the power of CPU/GPU cores nowadays, salting the password will not be a sufficient solution for a long time [13].

According to several experiments made since the late 60s by cognitive psychologists, these experiments have proven the pictorial superiority effect in a human. Accordingly, humans have extensive and exceptional abilities in remembering pictures [14]. In other words, the ability of the human brain in recognizing or recalling images is superior to its ability in recalling textual information where this has been acknowledged by psychology studies [15][16][17][18][19][20][21]. Based on this observation, graphical-based authentication has been proposed as an alternative authentication mechanism for the text-based authentication as graphical password mechanisms started to appear beginning around 1999 [15].

In addition to graphical-based authentication, another promising family of knowledge-based authentication is question-based techniques, in terms of their security and usability features. Questions based on user-related information can be used as an authentication method. For example, email service providers commonly use challenge question-based authentication for credential recovery [22].

In this paper, we propose a hybrid authentication method making use of both graphical-based and question-based approaches, with security and usability enhancement considerations. The related literature is surveyed and acknowledged in the next section. Then, a description of a user study conducted to evaluate the proposed approach is presented. We conclude the paper with some thoughts for future research in the area.

Manuscript received April 5, 2020
Manuscript revised April 20, 2020

2. Literature review

In this section, we review some studies that propose alternative solutions to traditional password-based authentication. In particular, we shed light on studies that focus on usability and security aspects. For example, Katsini et al. (2016) [23] presented a comprehensive review of the latest studies in knowledge-based authentication in the perspective of security and usability with the goal of improving authentication methodologies in these two aspects. From an empirical point of view, Vuksanovic and Al-Sinani (2009) [24], developed an image-based authentication system of the students' portals at the University of Portsmouth, which is called H-IBAS-H. They also proposed a knowledge-based authentication method as an additional stage besides an Intrusion Detection (ID) feature in which both of them work as improvements to increase the system's security without affecting its usability.

Ullah, Xiao and Lilley (2012) [25] reviewed benefits and constraints of traits of various authentication methods and their feasibility in the authentication process of students in an online examination environment. They proposed a knowledge-based solution for the purpose of student authentication process during online examinations called profile-based authentication framework (PBAF). In a subsequent study (2014) [26], they developed a hybrid approach which utilizes knowledge-based authentication mechanisms to enhance the usability and security of the authentication challenge questions of the online examination environment. They implemented an abuse case scenario.

Similarly, Schlöglhofer and Sametinger (2013) [27] have proposed a novel authentication system that combined mechanisms of authentication for Android to meet the security and usability requirements. Along similar lines, Takada and Ishizuka (2015) [28] proposed Chameleon Dial (CDial), which is a secured authentication system against CrA that is based on Personal Identification Number (PIN). In addition, Shaju et al. (2016) [29] proposed a three-factor authentication system consisting of a new authentication algorithm called Biometric-IMEI & SIM-Color (BISC), which enhances the security aspect of user authentication.

Skracic, Pale and Kostanjcar (2017) [30] proposed a new knowledge-based authentication approach that is based on non-public data sources that offer dynamical data sets, which change over time to generate unique challenge questions. The proposed approach was tested using different non-public data sources. Many other studies present various authentication solutions, which cannot be fully covered due to space limitations.

3. The proposed approach

The intuition behind this research is that improvements in usability can enhance the security of systems in general and authentication solutions in particular [15]. Therefore, a hybrid authentication system has been implemented as an alternative to the traditional password-based authentication which is currently used in students' portal at Umm Al-Qura University, with an aim to improve security and usability. The hybrid authentication system consists of two authentication layers.

The first layer is an image-based authentication phase, which is a cued-recall "locimetric" scheme, where the students are given a sequence of three images one at a time and they have to select one click point on each of these images. In order to be authenticated to the system, the three images will be presented to them in sequence and they have to click the pre-chosen click-points within the limits of a predefined tolerance area. The student has three attempts in the image-based authentication part. If an entry error occurs in one image, the student has to re-enter the three click-points again without informing the student where the error has occurred. The cued-recall scheme aims to help students in remembering their passwords [15][31] where the utilized image works as memory cue to aid users in recalling the click-points' locations in the three images, thus, increase the usability. On the other hand, the number of images utilized will increase the theoretical space of the password, subsequently, increase the security level of the system. The aim of the tolerance area is making the cued-recall methods usable as it is unrealistic that students click the exact selected pixel representing the password click-point. The tolerance area has an adjustable space value which can be adjusted according to security requirements. Students will never receive feedback on their wrong entries. This will increase the security of the system as it will be discussed in the results section.

The second layer is a question-based authentication phase, where the students are required to answer two challenge questions right after completing the image-based authentication part. University Students Database is perfect to be utilized in creating dynamic challenge questions, which can be used only once to increase security. The students have one attempt for each question. Using two questions instead of one question in the question-based authentication part supposed to increase the security level of the system as well. The main goal behind using two authentication schemes is to achieve high security levels and build various security layers so that each authentication layer can compensate the weakness of the other one.

4. Evaluation

We conducted two web-based user studies where the server recorded the login attempts over 4 weeks. The first study aims to compare the traditional text-based authentication with the proposed authentication system in term of usability. The second study aims to study the security of the proposed authentication system. 49 students were involved in this experiment. The participants are undergraduate students of Faculty of Computers and Information Systems at Umm Al-Qura University enrolled in the same course, hence they are familiar to each other.

Based on security and usability evaluation metrics, which have been defined and widely applied in the literature, we utilized three metrics. Regarding the usability, the metrics were as follows. First, efficiency, which refers to the speed of the authentication process. Second, effectiveness, which refers to the memorability of the password where its measured by the number of wrong entries. Third, user satisfaction, which is measured by a questionnaire.

Regarding security, the metrics were as follows. First, guessability, where the attacker guesses the password randomly or based on the direct or indirect knowledge about the legitimate user. Second, observability, where the attacker observed a legitimate authentication session to utilize the observed information to authenticate him/herself as a legitimate user. Third, recordability, where the attacker recording multiple legitimate authentication sessions to analyze them in order to be able to authenticate him/herself as a legitimate user.

To evaluate the usability, users logged in weekly into the two authentication systems, which are the text-based and the proposed hybrid one. To evaluate the security, the students were divided into groups of two students. To evaluate the guessability attack, each one of the two students guess the password of the other. To evaluate the observability attack, each one of the two students physically observe the authentication session of the other and try to replicate it as a legitimate user. To evaluate the recordability attack, each one of the two students try to authenticate as a legitimate user based on analyzing the video records of many authentication sessions of each of them.

5. Findings

5.1 Usability Analysis

5.1.1 Efficiency Analysis

	Week no.1			Week no.2			Week no.3			Week no.4		
	Arithmetic mean	Min	Max	Arithmetic mean	Min	Max	Arithmetic mean	Min	Max	Arithmetic mean	Min	Max
The first image	0.67	0.1	0.7	0.83	0.1	2.4	0.94	0.11	3.31	0.96	0.12	3.16
The second image	0.84	0.12	3.58	0.88	0.1	3.19	0.71	0.1	1.57	0.56	0.1	1.53
The third image	0.7	0.1	1.54	0.68	0.1	3.23	0.63	0.1	1.9	0.72	0.1	3.49
Image-based part	1.38	0.13	3.24	1.45	0.1	3.3	1.74	0.1	3.7	1.52	0.12	3.6
The first question	0.97	0.1	2.9	0.86	0.1	2.31	0.88	0.1	2.5	0.88	0.1	3.3
The second question	0.71	0.1	1.57	1.14	0.1	3.9	0.85	0.11	2.9	0.79	0.1	3.27
Question-based part	1.32	0.17	3.24	1.59	0.12	3.45	1.48	0.12	3.6	1.52	0.12	3.48
The Hybrid system	3.27	2.11	6.56	2.5	0.27	5.5	3.79	2.25	6.26	3.29	0.3	5.2
Text-based password	0.95	0.1	3.21	0.78	0.1	2.44	0.99	0.1	3.42			

Fig. 1 A comparison between authentication approaches in term of their efficiency

The arithmetic mean in the case of image-based passwords in each picture individually is better than text-based passwords. Comparing it to the sum of the three pictures, the difference is considered very acceptable. However, we should note that the login time in image-based password of the sum of the three pictures is affected by the occurrence of a wrong entry in any of the three pictures, as this necessitates the re-login of all three images again. The memorability issue in users was not affecting the time spent on the process of login where error rates on login was decreasing over time and the success rate was almost constant as will be explained later in memorability analysis section. If we take the previous observation into consideration besides the fact that the students use the image-based authentication for the first time, we expect that the time users spent on the process of login will improve over time with the improvement in their abilities of using the system correctly but this needs to be studied in the long term. The time taken to login is an important measure, but the success rate in answering the questions plays an important role as well.

The arithmetic mean in question-based passwords in each question individually is better than it in the text-based passwords but considered somewhat high for the sum of the two questions. This is due to memorability issues. As shown in the Figure 2, the arithmetic mean of the hybrid authentication system will drop clearly if we use one question only instead of two questions. Knowing that the hybrid authentication systems no.2 and no.3 consist of image-based authentication part beside question-based authentication part, which consists of one question only.

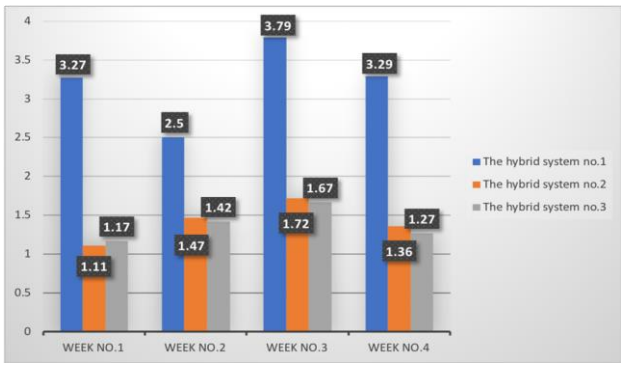

Fig. 2 The arithmetic means for the period of time it took students during the login process of the three hybrid authentication systems weekly.

5.1.2 Effectiveness Analysis

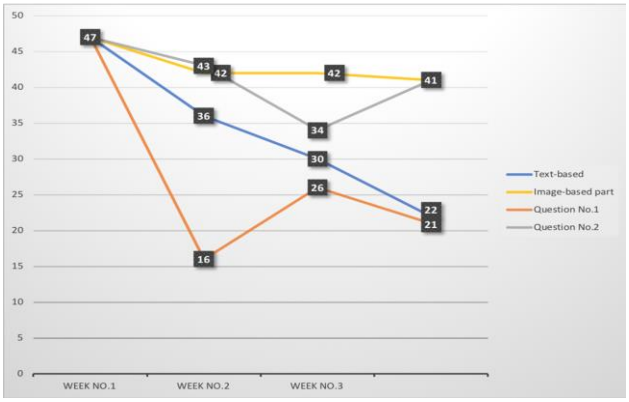

Fig. 3 A comparison between text-based, image-based and question-based authentication in the number of students who have succeeded in login

In text-based authentication, 23% of the students forgot their passwords from the first week. Also, we notice that the success rate in login was decreasing over time where the number of the students who forgot their passwords keep increasing over time, despite that 69% of them used a text-based password that they had previously used. Moreover, the error rate, which is the number of the entry errors, was increasing over time.

In image-based authentication, 11% of the students forgot their passwords from the first week. Also, we notice that the success rate in login was almost constant over time where the percentage of the students who forgot their passwords was decreasing over time and almost non-existent. Moreover, the error rate was decreasing over time.

Regarding the question-based authentication part, 45% of students failed to answer the first question whereas just 18% of them failed answering the second question. This indicates the effect of the type of questions on the memorability in users in question-based authentication part. Therefore, the type of questions must be chosen very carefully in order to improve the success rate in login and keep the error rate at the lowest possible rate. To improve the usability, users may prefer to choose the questions type they will be asked. Figure 3 summarizes these findings.

Regarding the hybrid authentication system, the number of the students who have succeeded in login was very low due to the number of questions used and their type. Figure 4 shows an improvement in the number of students who have succeeded in the login when we used only one question for the authentication part instead of two. Moreover, the number of students who have succeeded in the login through the hybrid authentication system no.3 very significantly increased comparing to the hybrid authentication system no.1 and no.2 when we used a good question type.

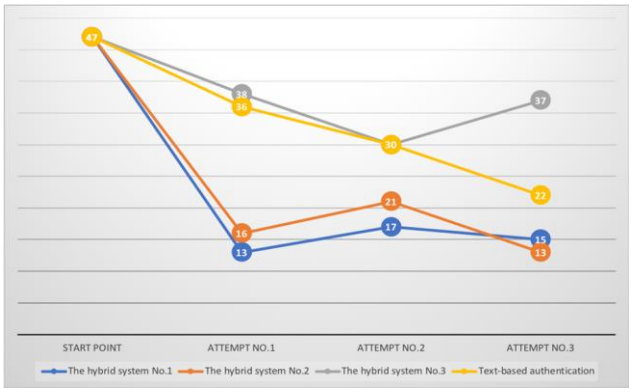

Fig. 4 A comparison between text-based authentication and the three hybrid authentication systems in the number of students who have succeeded in login.

5.1.3 User Satisfaction Analysis

I. Text-based authentication

Interestingly, 76% of students have mentioned that they often find it difficult to remember the text-based passwords for the systems they do not frequently login to. Also, 48% of them have mentioned that they believe that using the text-based password alone for the authentication is not secure, and 48% of them do not prefer using the text-based password alone for the authentication. However, some of them still prefer to use the text-based passwords in authentication for the following various reasons. First, some of the students prefer the text-based passwords because they find it easy to use in authentication since it is familiar to them despite that all of them was convinced that using text-based passwords alone in authentication is not secure. Second, the text-based passwords do not take time in authentication despite that all of the students who find it faster. Third, some of the students find text-based passwords memorable, knowing that all of the students who said that, are following wrong practices that help

them remember passwords like using one password for many applications where these practices affect the security of the systems.

II. The hybrid authentication system

64% of the students have mentioned that they found the image-based password easier to remember than the text-based passwords. Also, 56% of them believe that the hybrid authentication system is more secure than the text-based authentication and 88% of them believe that combining the image-based and question-based authentication into a hybrid authentication system will prevent the security issues that appear when they are used separately. Despite that, 46% of the students believe that combining the image-based and question-based authentication into a hybrid authentication system to improve the security will further complicate the system. Also, 56% of them prefer the hybrid authentication system over the text-based authentication.

However, 16% of the students still do not prefer the hybrid authentication system for the following various reasons. First, some of the students believe that the hybrid authentication system is not secure. Second, the text-based passwords are easier to remember than the image-based passwords. Third, the hybrid authentication system is complicated because it consists of two authentication parts. Fourth, using three pictures in the image-based authentication part beside the tolerance space complicates the usability of the hybrid authentication system. Fifth, it is difficult to remember the answers of the questions in the question-based authentication part. Finally, the hybrid authentication system takes long time to login compared to the text-based authentication.

5.2 Security Analysis

5.2.1 Guessability Analysis

Noticeably, 73% of guessing attempts were successful. However, no single attack has successfully occurred. This is due to the number of pictures used to be authenticated where using three pictures increase the password space, which in turn complicates the guessing attack. Also, not notifying the user of the correct or the wrong click points' locations in the three pictures during the authentication has complicated the guessing attack too.

5.2.2 Observability Analysis

The large percentage of the successful logins was in the image-based authentication part where the attacks occurred represents the percentage of 86%. However, the effect of using three pictures to be authenticated beside the effect of the tolerance space, have helped to reduce the impact of this type of the attack where the failed attempts was 14%. Moreover, the question-based authentication part has reduced the impact of this type of the attack on the hybrid authentication system in a large percentage where the failed attempts in the question-based authentication part was with a percentage of 93%. The attacks on the question-based authentication part were in the cases that the attackers have a strong knowledge on the legitimate students, thus, the answers were not random guesses or based on observing a previous legitimate login.

5.2.3 Recordability Analysis

The number of pictures to be authenticated and the tolerance space besides not notifying the user of the correctness of the click points' locations in the three pictures during the authentication had an effect to reduce the impact of this type of attacks. The question-based authentication part has reduced the impact of this type of attacks on the hybrid authentication system where the successful attacks on the hybrid system was 7%. This means that the attackers' strong knowledge about the legitimate users will not be effective enough to execute the attack on the question-based authentication part, but this needs further study.

5.2.4 Text-based password Analysis

Based on the analysis of the questionnaire results, all the students were resorting to wrong practices that help them remembering their text-based passwords. One of the most important of these wrong practices is to choose weak passwords and ignore the policies of the strong text-based passwords where the percentage of the weak passwords was 90%, knowing that 82% of these passwords have required four days as maximum to be cracked. Also, all of their theoretical spaces are short. Moreover, 69% of them were previously used for many applications. Also, among the strong passwords, 60% of them were previously used.

A large percentage of the students (54%) preferred to choose text-based passwords that encompass personal information as this help them to remember their passwords. Despite that, 78% of them have mentioned that they often committed to the strong passwords policies instructions. However, these strict policies not necessarily guarantee an adequate security for the authentication systems even if the passwords were strong enough for the following reasons. 64% of the students who find it difficult remembering the text-based passwords and committed to the strong passwords policies are using passwords that have been previously used. Also, 36% of them were writing down their passwords for easy reference and 36% of them are choosing permanent or temporary password saving options such as "remember me later" so they can login directly without the passwords in the subsequent sessions.

Regarding the strong passwords policies instructions, 56% of the students find that these policies complicate the text-based passwords and the ability to remember these

passwords in the long term. The rest of them were all resorting to wrong practices that help them in remembering their text-based passwords.

6. Discussion

Regarding usability, the utilized cued-recall scheme has shown a good memorability and efficiency. However, the tolerance space, which requires accuracy, is still an issue that affects the usability. The usability of the question-based authentication part is mainly depending on the question type. In general, the hybrid authentication system was preferred by a large percentage of the students compare to text-based password. However, its usability issues fall behind the number of the authentication steps beside the issues associated with the memorability in question-based authentication part where these two affect the efficiency of the system. Using one question instead of two in question-based part may reduce this issue. Also, we could use the question-based authentication part only when the student login from a new device.

Regarding security, the theoretical password space of the cued-recall scheme is large. Also, the cued-recall scheme appeared impervious to dictionary attacks more than the text-based passwords, which appeared vulnerable against it. However, it appears vulnerable against the observability and recordability attacks. Also, the security is mainly depending on the utilized authentication images. The hotspots issue is still remaining, thus, there is a need to use a Persuasive Technology, which aims to influence users' choices of click-points by encouraging users and guiding them to avoid selecting click-points which are hotspots, thus, creating secure passwords. Despite that the question-based authentication part appeared impervious against guessing, observability and recordability attacks, however, the security is mainly depending on the database, which is utilized to create the dynamic questions. In particular, it should be large enough to create one-time challenge questions. Also, the attacker should not be able to predict the answers to these questions based on public knowledge sources. To overcome the security issues of the hybrid authentication system, which come from the two authentication layers, it is preferred to use the two-factor authentication through the student's email when he/she login from a new device.

7. Conclusion and future work directions

This paper presented a hybrid authentication system as an alternative to the text-based password authentication. Also, it reports on the usability of the proposed system after analyzing the results of the user study. The hybrid authentication system appeared effective to be used as an alternative for the text-based password. Moreover, it showed many advantages in terms of security and usability and some of them showed superiority over the text-based passwords authentication. However, there still several limitations that need to be considered.

In future studies, we will explore ways to prevent the questions from being repeated as the academic record of the student is limited and will not be effective to create dynamic questions for one-time for long term.

References

[1] Almuairfi, S., Veeraraghavan, P., and Chilamkurti, N. 2011. IPAS: Implicit Password Authentication System. In IEEE Workshops of International Conference on Advanced Information Networking and Applications Workshops (Biopolis, Singapur, March 22 - 25, 2011). WAINA'11. IEEE, Piscataway, NJ, 430–435.

[2] M. D. Hafiz, A. H. Abdullah, N. Ithnin, and H. K. Mammi, "Towards identifying usability and security features of graphical password in knowledge based authentication technique," in Proceedings of the IEEE 2008 (AICMS 08), IEEE, 2008, pp. 396–403.

[3] K. Renaud, D. Kennes, J. Van Niekerk, and J. Maguire, "SNIPPET: Genuine knowledge-based authentication," in Information Security for South Africa, 2013, 2013, pp. 1–8.

[4] Dhamija, R., Perrig, A. 2000. Déjà Vu: a user study using images for authentication. In: Proceedings of the 9th Conference on USENIX Security Symposium (Denver, Colorado, August 14 - 17, 2000), 45-58.

[5] M. Kotadia, "Microsoft: Write down your passwords", In ZDNet, Australia, 2005.

[6] B. Riddle, M. Miron, and J. Semo, "Passwords in use in a university timesharing environment," Computers and Security, vol. 8, no. 7, pp. 569–578, 1989.

[7] A. Conklin, G. Dietrich, and D. Walz, "Password-based authentication: a system perspective," in System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on. IEEE, 2004, pp. 10–pp.

[8] D. Florencio, C. Herley, and B. Coskun, "Do strong web passwords accomplish anything?" in Proceedings of the 2nd USENIX workshop on Hot topics in security. USENIX Association, 2007, p. 10.

[9] P. J. Inglesant, and M. A. Sasse, "The true cost of unusable password policies: password use in the wild," in Proceedings of the 2010 SIGCHI Conference on Human Factors in Computing Systems (CHI '10). ACM, NY, USA, 2010, pp. 383-392.

[10] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman, "Of passwords and people: measuring the effect of password-composition policies," in Proceedings of the 2011 SIGCHI Conference on Human Factors in Computing Systems (CHI '11). ACM, New York, NY, USA, 2011, pp. 2595-2604.

[11] D. Klein, "Foiling the cracker: A survey of, and improvements to, password security," in Proceedings of the 2nd USENIX Security Workshop, Portland, Oregon, August 27, 1990, pp. 5-14.

[12] K. Gilhooly, "Biometrics: Getting Back to Business", in Computerworld, May 2005.

[13] F. Milo, M. Bernaschi, and M. Bisson, "A fast, GPU based, dictionary attack to OpenPGP secret keyrings," Journal of

Systems and Software, vol. 84, no. 12, pp. 2088–2096, Dec. 2011.
[14] R. Weiss, A. De Luca, “PassShapes: utilizing stroke based authentication to increase password memorability,” in Proceedings of the 2008 NordiCHI. ACM Press, 2008, pp. 383- 392.
[15] R. Biddle, S. Chiasson, and P. van Oorschot, 2012. “Graphical passwords: Learning from the first twelve years,” ACM Computing Surveys, 44(4), 41 pages.
[16] Bower, G. H., Karlin, M. B., & Dueck, A. (1975). Comprehension and Memory for Pictures. Memory and Cognition, 2, 216-220.
[17] Calkins, M. W. (1898) Short studies in Memory and Association from the Wellesley College Laboratory. Psychological Review, 5, 451-462.
[18] Paivio, A., Rogers, T. B., & Smythe, P. C. (1968) Why Are Pictures Easier to Recall Than Words? Psychonomic Science, 11, 137-138.
[19] Shepard, R. N. (1967). Recognition Memory for Words, Sentences, and Pictures. Journal of Verbal Learnings and Verbal Behavior, 6, 156-163.
[20] Standing, L. (1973). Learning 10,000 Pictures. Quarterly Journal of Experimental Psychology, 25, 207-222.
[21] E.A.Kirkpatrick,An experimental study of memory, Psychol. Rev. 1(6)(1894) 602.
[22] Schechter S., Brush A J. B., Egelman S., editors. It's No Secret. Measuring the Security and Reliability of Authentication via. 30th IEEE Symposium on Security and Privacy; 2009: IEEE.
[23] C. Katsini, M. Belk, C. Fidas, N. Avouris, and G. Samaras, “Security and usability in knowledge-based user authentication: A review,” in Proceedings of the 20th Pan-Hellenic Conference on Informatics (PCI ’16), ACM, New York, NY, USA, 2016, pages 63:1–63:6
[24] B. Vuksanovic, H. Al-Sinani, “Two Proposals for Improving the Image-Based Authentication System: H-IBAS-H,” In: First International Conference on Evolving Internet, IEEE, 2009, pp. 168–171.
[25] A. Ullah, H. Xiao and M. Lilley, "Profile based student authentication in online examination," International Conference on Information Society (i-Society 2012), London, 2012, pp. 109-113.
[26] A. Ullah, H. Xiao, T. Barker, M. Lilley, "Graphical and Text Based Challenge Questions for Secure and Usable Authentication in Online Examinations". The 9th International Conference for Internet Technology and Secured Transactions (ICITST), 2014, London, UK: IEEE.
[27] Schlöglhofer, R., & Sametinger, J. 2012. Secure and usable authentication on mobile devices. In Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia. ACM, 257-262.
[28] Tetsuji Takada and Masaya Ishizuka. 2015. Chameleon dial: repeated camera-recording attack resilient PIN input scheme. In Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers (UbiComp/ISWC’15 Adjunct). Association for Computing Machinery, New York, NY, USA, 365-368. DOI:https://doi.org/10.1145/2800835.2800905
[29] S. Shaju and Panchami V, "BISC authentication algorithm: An efficient new authentication algorithm using three factor authentication for mobile banking," 2016 Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, 2016, pp. 1-5.
[30] Skrai K, Pale P, Kostanjar Z. Authentication approach using one-time challenge generation based on user behavior patterns captured in transactional data sets. Comput Secur 2017;67(Suppl C):107–21.
[31] CHIASSON, S., VAN OORSCHOT, P. C., AND BIDDLE, R. 2007b. Graphical password authentication using Cued Click Points. In Proceedings of the European Symposium on Research in Computer Security (ESORICS). Lecture Notes in Computer Science, vol. 4734, Springer, Berlin, 359–374