An Analysis of Graphical User Authentication Systems

Yean Li Ho, Afizan Azman, Siong Hoe Lau
Faculty of Information Science and Technology
Multimedia University
Melaka, Malaysia
{ylho;afizan.azman;lau.siong.hoe}@mmu.edu.my

***Abstract*— Since 1996, when Blonder [1] proposed the first graphical user authentication (GUA) system, there have been many graphical password systems proposed as an alternative to the textual password system used in most authentication systems today. However, these GUA systems have not been evaluated using a single common framework. The purpose of this paper is to analyse and assess existing Graphical User Authentication (GUA) systems which are available in the existing literature based on a common framework, the Usability-Deployability-Security(UDS) Framework proposed by Bonneau et al. [2].**

Keywords—graphical passwords ; graphical user authentication; UDS framework ; human computer interface security

I. INTRODUCTION

A study done by Adams, Sasse and Lunt [3] revealed that 50% of the people tested using the common textual password wrote down their passwords because it was too difficult to remember. This defeats the purpose of having a password because their exposed password could easily be used by an unauthorized person to access their account which is supposed to be protected by their password. Hence, the graphical user authentication (GUA) system was introduced as an alternative solution because it is supposed to be more usable and easier to remember. However, these GUA systems have their own issues as will be shown by this paper.

II. CATEGORIZATION OF GUAS

There are many ways of categorizing the GUA systems. Some literature like Suo, Zhu and Owen [4] and Biddle, Chiasson and van Oorschot [5] have attempted to categorize the GUAs but their list is not complete and up to date today. We have re-categorized the existing GUAs with a list of 90 existing GUAs since 1996 as shown in Figure 1. We propose four main categories: Recognition-based GUAs, Recall-Based GUAs, Recognition-Recall based Hybrid GUAs and Textual-Graphical Hybrid GUAs.

Recognition-Based GUAs are GUAs which allows a user to recognize his or her password based on given clues. They are also known as Searchmetric or Cognometric GUAs [6][7]. They usually contain multiple images and requires a user to recognize and select an image from the choices given.

Recall-Based GUAs are GUAs which require the user to recall or remember the password from scratch instead of selecting it from a given list of options. These GUAs can be subdivided into two categories: Pure Recall GUAs or Cued Recall (also known as Iconmetric) GUAs.

Pure Recall GUAs are also known as Drawmetric GUAs [6][7] because they require a user to draw the password from scratch. This type of GUA system can be divided into Grid-Based or Non-Grid-Based GUAs.

Cued Recall GUAs however, require the user to recall their password when they are given a cue or a clue which is supposed to jog the memory of the user and aid him or her to remember the actual password. We propose to re-categorise these GUAs as Locimetric and Psychometric GUAs. Locimetric GUAs [6][7] are usually location sensitive whereby the system detects the password based on certain locations which are selected on the screen in order to form the password. We then propose to sub-divide Locimetric GUAs into Single-Image and Multiple Image GUAs.

There is only one Psychometric GUA system which was proposed by Stubblefield and Simon in 2004 [8]. This system is so named because it requires a user to think of the first word which comes to mind when given a picture of inkblots. This method is based on the fact that different users can interpret random, undefined images differently so the psychology of each individual is unique.

The Recognition-Recall based Hybrid GUA is a GUA system which combines the recognition properties of the Recognition-based GUA with the Recall properties of a Recall-based GUA. There are currently nine types. The first one, the Association-based Graphical Password was introduced in 2005 by Li et al.[9].

Finally, the last category is the Textual-Graphical Hybrid GUA. This type of GUA combines the properties of a textual password with the properties of the graphical password. This category is probably the easiest category to transition to from the original common textual password system because it makes use of the original textual password and combines it with graphical password properties to make it easier to remember. There are currently 20 different types of textual-graphical hybrid GUAs in existence today since 2003.

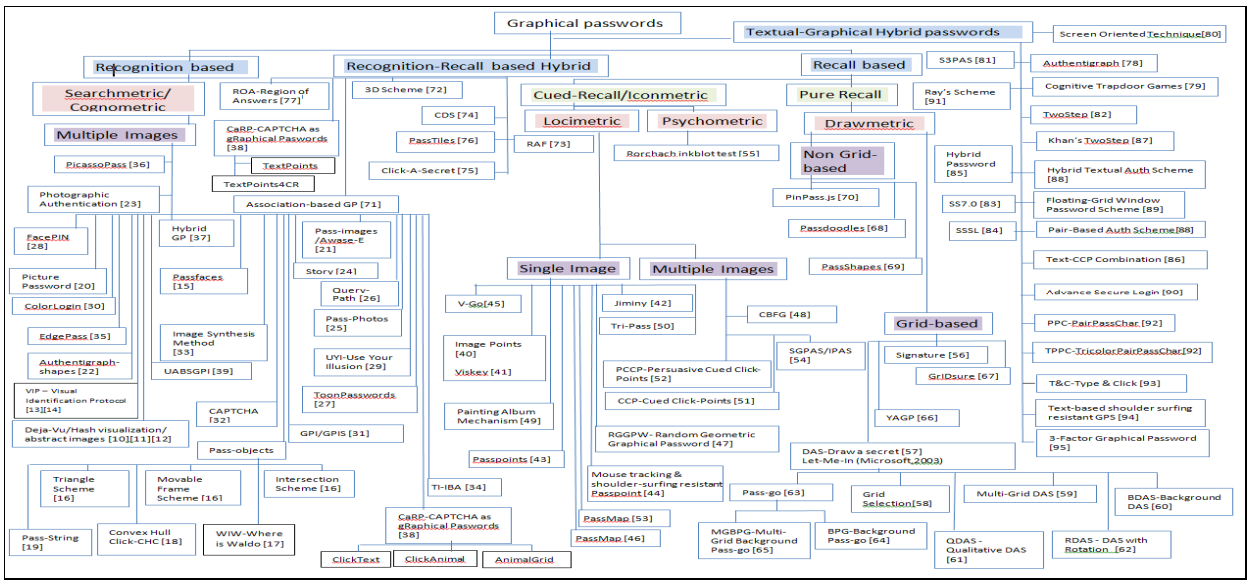

Figure 1: Categorization of Graphical User Authentication Systems

III. Evaluation Methods

There is no common framework used for evaluation of each of the 90 graphical user authentication systems listed. Figure 2 shows the types of methods used to evaluate the graphical user authentication systems as listed in Figure 1.

The most frequently used method is to measure the amount of time taken to log into the authentication system. This is equivalent to the speed of entry into the system. This is used to measure the usability of the graphical user authentication system. The most frequent choice of measuring the security of the graphical user authentication system is to calculate the password space of the graphical user authentication system. Other commonly used methods of evaluating the usability of the GUAs include measuring the login success and failure rate of the participants, issuing questionnaires and conducting a user study by observing how the users use the GUA. Some of the statistical methods used to measure usability include t-tests, Chi-square test, ANOVA, Kruskal-Wallis, Newman-Keul, Wilcoxon, J-statistics, F-Tests, MRT and Mann-Whitney.

A qualitative evaluation of the most common security issues affecting all the 90 different types of graphical user authentication systems reveals that the most common security issues are shoulder-surfing, dictionary attack, brute force attack, guessing and man-in-the-middle attack. It appears that the most secure GUA is EdgePass [35] and CBFG [48], which are resistant to all attacks listed and the most unsecure GUA is Pass-Photos [25] and Text-CCP Combination [86] which are susceptible to attack from all of the attacks listed. Almost all the recognition-based GUA and the Drawmetric GUA are susceptible to man-in-the-middle attacks.

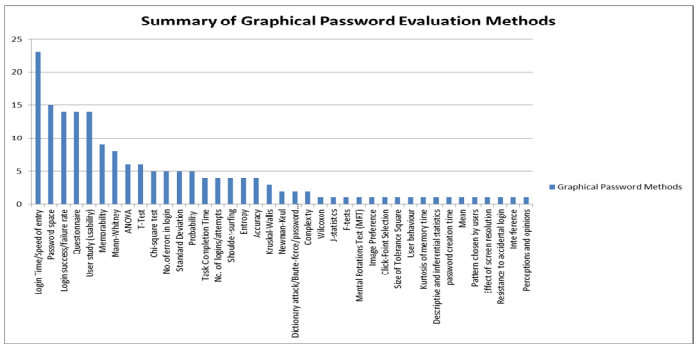

Figure 2: Summary of Graphical Password Evaluation Methods

IV. Usability-Deployability-Security (UDS) Framework

Bonneau et al. [2] proposed a framework to evaluate authentication systems as shown in Figure 3. This framework was originally used to evaluate web authentication systems. However, we have applied this qualitative framework to evaluate all the existing GUAs as shown in Table 1.

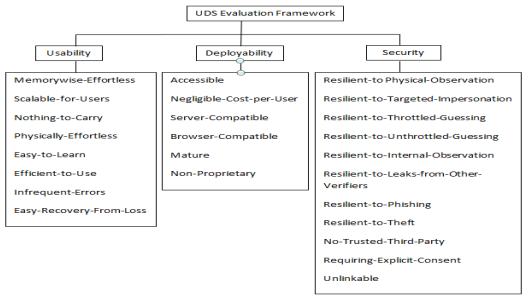

Figure 3 : Usability-Deployability-Security (UDS) Framework

We refer the reader to [2] for a detailed definition of each criterion in the UDS Evaluation Framework.

The analysis shows that in order to deploy the GUAs, most of the GUAs require a lot of work and effort to make the transition from textual password to the proposed GUA. Therefore, these GUAs are weak in terms of server compatibility, browser-compatibility and maturity. The analysis also shows that accessibility to most of the GUA systems by users who are physically impaired in some way is poor as there is no support given for the visually impaired or the physically impaired users especially in recall-based GUAs and its variants.

In terms of security, most of the GUAs are protected from impersonation. This is due to the fact that it is difficult to describe to another user one's graphical password because of the nature of the password. In this sense, graphical passwords are more secure than textual passwords. Subsequently, most GUAs are resilient to phishing and theft. They are also resilient to leaks from other verifiers. This means that nothing that is leaked can help an attacker impersonate a legitimate user. These GUAs also do not require a trusted third party to function, therefore it is safe from exposure to attacks on a third party in order to obtain the passwords. Also, the authentication process of all GUAs cannot begin without the explicit consent and action of a user (unlike RFID cards). All GUAs are also unlinkable in that no connection can be made between the logins of two separate accounts by the same user. This protects the privacy of the user.

V. Conclusion

This paper gives an overview of all the existing graphical user authentication system to date. This purpose of this paper is to re-categorize all the existing GUAs and to analyse all the existing GUAs using a common framework by applying the UDS framework to assess all the graphical user authentication systems available to date.

References

[1] Blonder, G. "Graphical password". U.S. patent 5,559,961, field August 30, 1995, and issued September 24, 1996

[2] Bonneau, J., Herley, C., Van Oorschot, P.C. & Stajano, F, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes", Security and Privacy (SP), 2012 IEEE Symposium on, pp. 553-567, 2012.

[3] Adams, A., Sasse, M.A., & Lunt, P., "Making Passwords Secure and Usable", HCI 97 Proceedings of HCI on People and Computers XII, pp. 1-19, 1997.

[4] Suo, X., Zhu, Y. and Owen, G.S., "Graphical Passwords:A survey", ACSAC '05 Proceedings of the 21st Annual Computer Security Applications Conference, pp. 463 – 472, 2005.

[5] Biddle, R., Chiasson, S., & Oorschot, P. C. Van., "Graphical Passwords: Learning from the First Twelve Years". Technical Report TR-11-01, School of Computer Science, Carleton University,pp.1-25, 2011.

[6] De Angeli, A., Coventry, L., Johnson, G., & Renaud, K., "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems", International Journal of Human-Computer Studies, 63(1-2), 128–152. doi:10.1016/j.ijhcs.2005.04.020, 2005.

[7] Everitt, K. M., Bragin, T., Fogarty, J., & Kohno, T., "A Comprehensive Study of Frequency , Interference , and Training of Multiple Graphical Passwords", Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'09), pp. 889–898, 2009.

[8] Stubblefield, A. & Simon, D. R., "Inkblot Authentication". Technical Report MSR-TR-2004-85.1–16, 2004.

[9] Li, Z., Sun, Q., Lian, Y., Giusto, D. D., & Star, A., "An Association-Based Graphical Password Design Resistant To Shoulder-Surfing Attack", IEEE International Conference on Multimedia and Expo 2005 (ICME 2005), pp. 2–5, 2005.

[10] Dhamija, R., & Perrig, A., "Déjà Vu : A User Study Using Images for Authentication", Human Factors, (102590), 4. Retrieved from http://portal.acm.org/citation.cfm?id=1251306.1251310, 2000.

[11] Perrig, A. & Song, D., "Hash Visualization : a New Technique to improve Real-World Security", International Workshop on Cryptographic Techniques and E-Commerce, pp. 1–8, 1999.

[12] Dhamija, R., "Hash visualization in user authentication", CHI '00 Extended Abstracts on Human Factors in Computer Systems (CHI '00). 279-280. doi:10.1145/633451.633455, 2000.

[13] Angeli, A. De, Coutts, M., Coventry, L.,& Johnson, G. I., "VIP : a visual approach to user authentication". AVI2002,pp. 316–323, 2002.

[14] Angeli, A. De, Coventry, L., Johnson, G., & Coutts, M., "Usability And User Authentication : Pictorial Passwords Vs . PIN", Contemporary Ergonomics 2003, pp. 253-258, 2003.

[15] Sobrado, L. & Birget, J.C., "Graphical passwords". The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, 2002.

Table 1: Evaluation of GUAs using UDS Framework

No	GP System	Usability: Memorywise-Effortless	Usability: Scalable-for-Users	Usability: Nothing-to-Carry	Usability: Physically-Effortless	Usability: Easy-to-Learn	Usability: Efficient-to-Use	Usability: Infrequent-Errors	Usability: Easy-Recovery-From-Loss	Deployability: Accessible	Deployability: Negligible-Cost-per-User	Deployability: Server-Compatible	Deployability: Browser-Compatible	Deployability: Mature	Deployability: Non-Proprietary	Security: Resilient-to-Physical-Observation	Security: Resilient-to-Targeted-Impersonation	Security: Resilient-to-Throttled-Guessing	Security: Resilient-to-Unthrottled-Guessing	Security: Resilient-to-Internal-Observation	Security: Resilient-to-Leaks-From-Other-Verifiers	Security: Resilient-to-Phishing	Security: Resilient-to-Theft	Security: No-Trusted-Third-Party	Security: Requiring-Explicit-Consent	Security: Unlinkable
Recognition-Based GUA - Searchmetric/Cognometric																										
1	Deja-Vu / Hash visualization / Abstract images [10], [11],[12]	×	×	√	×	√	○	○	√	×	√	×	×	×	√	×	√	×	×	×	√	√	√	√	√	√
2	Passfaces [15]	×	×	√	×	√	○	○	√	×	√	×	×	√	×	×	○	×	×	×	√	√	√	√	√	√
3	VIP-Visual Identification Protocol [13],[14]	×	×	√	×	√	○	○	√	×	√	×	×	×	√	×	○	×	×	×	√	√	√	√	√	√
4	Pass-objects - Triangle Scheme [16]	×	√	√	×	√	×	×	√	×	√	×	×	×	√	√	√	√	√	×	√	√	√	√	√	√
5	Pass-objects - Movable Frame Scheme [16]	×	√	√	×	×	×	×	√	×	√	×	×	×	√	√	√	√	√	×	√	√	√	√	√	√
6	Pass-objects - Intersection Scheme[16]	×	√	√	×	×	×	×	√	×	√	×	×	×	√	√	√	√	√	×	√	√	√	√	√	√
7	WIW-Where is Waldo [17]	×	√	√	×	×	×	×	√	×	√	×	×	×	√	√	√	√	√	×	√	√	√	√	√	√
8	Picture Password [20]	×	×	√	×	×	√	○	√	×	√	×	×	×	√	×	√	×	×	×	√	√	√	√	√	√
9	Pass-images / Awase-E [21]	×	×	√	×	×	√	○	√	×	√	×	×	×	√	×	√	×	×	×	√	√	√	√	√	√
10	Authentigraph-Shapes [22]	×	○	√	×	×	√	○	√	×	√	×	×	×	√	×	√	×	×	×	√	√	√	√	√	√
11	Photographic Authentication [23]	×	√	√	×	×	√	○	√	×	√	×	×	×	√	×	×	×	×	×	×	○	○	○	√	√
12	CHC- Convex Hull Click [18]	×	√	√	×	×	×	×	√	×	√	×	×	×	√	√	√	√	√	√	√	√	√	√	√	√
13	Story scheme [24]	×	√	√	×	×	√	○	√	×	√	×	×	×	√	×	○	×	×	×	×	○	○	√	√	√
14	Pass-String [19]	×	√	√	×	×	×	×	√	×	√	×	×	×	√	√	√	√	√	√	√	√	√	√	√	√
15	Pass-Photos [25]	×	√	√	×	×	×	○	√	×	√	×	×	×	√	×	×	×	×	×	×	○	○	√	√	√
16	Query-Path [26]	×	×	√	×	×	×	×	×	×	√	×	√	√	×	○	√	×	×	×	√	√	√	√	√	√
17	ToonsPasswords [27]	×	×	√	×	√	√	○	√	×	√	×	×	×	√	×	○	×	×	×	√	√	√	√	√	√
18	FacePIN [28]	×	√	√	×	√	√	○	√	×	√	×	×	×	√	×	○	×	×	×	√	√	√	√	√	√
19	UVI - Use Your Illusion [29]	^	√	√	√	^	√	^	√	^	√	^	^	^	√	√	√	√	√	^	√	√	√	√	√	√
20	ColorLogin [30]	×	√	√	×	×	√	○	√	×	√	×	×	×	√	×	√	√	√	×	√	√	√	√	√	√
21	GPI/GPIS [31]	×	√	√	×	×	×	×	√	×	√	×	×	×	√	×	√	×	×	×	√	√	√	√	√	√
22	CAPTCHA [32]	×	√	√	×	×	×	×	√	×	√	×	×	×	√	√	√	√	√	×	√	√	√	√	√	√
23	Image Synthesis Method [33]	×	√	√	×	×	√	○	√	×	√	×	×	×	√	√	√	√	√	×	√	√	√	√	√	√
24	Authentication [34]	×	√	√	×	×	×	×	√	×	√	×	×	×	√	√	√	√	√	×	√	√	√	√	√	√
25	EdgePass [35]	√	√	√	×	×	×	×	√	×	√	×	×	×	√	√	√	√	√	×	√	√	√	√	√	√
26	PicassoPass [36]	×	√	√	×	×	√	×	○	×	√	×	×	×	√	×	√	×	×	×	√	√	√	√	√	√
27	Hybrid Graphical Password [37]	×	√	√	×	×	√	×	○	×	√	×	×	×	√	×	√	×	×	×	√	√	√	√	√	√
28	CaRP (Captcha gRaphical Password) – ClickText [38]	×	√	√	×	×	√	√	×	×	√	×	×	×	√	×	√	×	×	×	×	√	×	√	√	√
29	CaRP (Captcha gRaphical Password) – ClickAnimals [38]	×	√	√	×	×	√	√	○	×	√	×	×	×	√	×	√	×	×	×	×	√	√	√	√	√
30	CaRP (Captcha gRaphical Password) – AnimalGrid [38]	×	√	√	×	×	×	×	√	×	√	×	×	×	√	×	√	×	×	×	×	√	√	√	√	√
31	UABSGPI -User Authentication By Secured Graphical Password Implementation [39]	×	√	√	×	○	×	○	√	×	√	×	×	×	√	×	√	×	×	×	×	√	√	√	√	√
Recall-Based GUA - Cued Recall - Locimetric - Single Image																										
32	Image Points [40],[41]	×	√	√	×	√	√	√	×	×	√	×	×	√	×	×	√	√	√	×	√	√	√	√	√	√
33	Jiminy [42]	×	√	√	×	×	○	×	○	√	×	×	×	×	√	×	√	○	×	×	√	√	√	√	√	√
34	Passpoints [43]	×	√	√	×	×	○	×	√	×	√	×	×	×	√	×	√	○	×	×	√	√	√	√	√	√
35	Mouse tracking & shoulder-surfing resistant Passpoint [44]	×	√	√	×	×	○	×	√	√	×	√	×	×	√	√	√	×	×	×	√	√	√	√	√	√
36	V-Go [45]	×	×	√	×	×	○	×	○	√	×	√	×	×	√	×	√	×	×	×	○	√	√	√	√	√
37	PassMap [46]	×	√	√	×	×	×	×	√	×	√	×	×	×	√	×	√	×	×	×	×	√	√	√	√	√
38	RGGPW- Random Geometric Graphical Password [47]	×	√	√	×	×	○	×	√	×	√	×	×	×	√	×	√	×	×	×	√	√	√	√	√	√
39	Painting Album Mechanism [49]	×	×	√	×	√	√	√	×	×	√	×	×	×	√	×	√	×	×	×	○	√	√	√	√	√
40	Tri-Pass [50]	×	×	√	×	×	×	×	√	×	√	×	×	×	√	○	√	×	×	×	√	√	√	√	√	√
Recall-Based GUA - Cued Recall - Locimetric - Multiple Images																										
41	CCP-Cued Click Points [51]	×	×	√	×	√	○	×	√	×	√	×	√	×	√	×	√	○	×	×	√	√	√	√	√	√
42	PCCP-Persuasive Cued Click-Points [52]	×	×	√	×	√	○	×	√	×	√	×	√	×	√	×	√	○	×	×	√	√	√	√	√	√
43	CBPG – Click Buttons according to Figures in Grids [	×	√	√	×	×	×	○	√	×	√	×	×	×	√	×	√	○	×	×	√	√	√	√	√	√
44	PassMap [53]	×	√	√	×	×	√	○	×	√	×	√	×	×	√	×	√	×	×	×	○	√	√	√	√	√
45	Authentication System /IPAS- Implicit Password Authentication System [54]	×	√	√	×	○	×	○	√	×	√	×	×	×	√	×	√	×	×	×	×	√	√	√	√	√
Recall-Based GUA - Cued Recall - Psychometric																										
46	Rorchach inkblot test [55]	×	√	√	×	√	○	○	√	×	√	×	√	×	×	√	√	×	×	√	○	√	√	√	√	√
Recall-Based GUA - Pure Recall - Drawmetric - Non Grid-Based																										
47	Passdoodles [68]	×	√	√	×	√	○	○	√	×	√	×	×	×	√	×	√	×	×	×	○	√	√	√	√	√
48	PassShapes [69]	×	×	√	×	√	√	√	×	×	√	×	×	×	√	×	√	×	×	×	×	√	×	√	√	√
49	pinPass.js [70]	×	×	√	×	√	○	○	√	×	√	×	×	×	√	×	√	×	×	×	○	√	√	√	√	√
Recall-Based GUA - Pure Recall - Drawmetric - Grid-Based																										
50	Signature [56]	×	√	√	×	√	○	×	√	×	√	×	×	×	√	×	√	○	○	×	×	√	√	√	√	√
51	DAS-Draw a secret [57]	×	○	√	×	√	○	×	√	×	√	×	×	√	×	×	√	×	×	×	×	√	√	√	√	√
52	Grid Selection [58]	×	√	√	×	√	×	×	√	×	√	×	×	×	√	×	√	×	×	×	×	√	√	√	√	√
53	Multi-Grid DAS [59]	×	√	√	×	√	×	×	√	×	√	×	×	×	√	×	√	×	×	×	×	√	√	√	√	√
54	BDAS -Background DAS [60]	×	×	√	×	√	×	×	√	×	√	×	×	×	√	×	√	×	×	×	×	√	√	√	√	√
55	QDAS - Qualitative DAS [61]	×	√	√	×	√	×	×	√	×	√	×	×	×	√	×	√	×	×	×	×	√	√	√	√	√
56	RDAS - DAS with Rotation [62]	×	√	√	×	√	×	×	√	×	√	×	×	×	√	×	√	×	×	×	×	√	√	√	√	√
57	Pass-go [63]	×	√	√	×	√	○	○	×	×	√	×	×	√	×	×	√	×	×	×	×	√	√	√	√	√
58	BPG – Background Pass-Go [64]	×	√	√	×	√	○	○	√	×	√	×	×	√	×	×	√	×	×	×	×	√	√	√	√	√
59	MGBPG – Multi-Grid Background Pass-Go [65]	×	√	√	×	√	○	○	√	×	√	×	×	√	×	×	√	×	×	×	×	○	√	√	√	√
60	YAGP-Yet Another Graphical Password [66]	×	√	√	×	√	○	○	√	×	√	×	×	√	×	×	√	×	×	×	×	○	√	√	√	√
61	GridSure [67]	×	×	√	×	√	○	○	√	×	√	×	√	×	√	×	√	×	×	×	×	√	√	√	√	√
Recall and Recognition Based Hybrid GUA																										
62	Association-based Graphical Password [71]	×	√	√	×	√	○	×	√	×	√	×	×	×	√	○	√	×	×	×	○	○	○	√	√	√
63	3D-Scheme [72]	×	√	√	×	×	×	×	√	×	√	×	×	×	√	×	√	×	×	×	○	√	○	√	√	√
64	RAF - Recall a Formation [73]	×	√	√	×	√	○	○	√	×	√	×	×	×	√	×	√	×	×	×	○	√	○	√	√	√
65	CDS [74]	×	○	√	×	√	○	○	√	×	√	×	×	×	√	×	√	×	×	×	√	○	○	√	√	√
66	Click-A-Secret [75]	×	×	√	×	√	○	○	√	×	√	×	×	×	√	×	√	×	×	×	√	√	○	√	√	√
67	PassTiles [76]	×	×	√	×	√	○	○	√	×	√	×	×	×	√	×	√	×	×	×	√	√	○	√	√	√
68	ROA-Region of Answers [77]	×	√	√	×	√	×	×	√	×	√	×	×	×	√	×	√	×	×	×	√	√	○	√	√	√
69	CaRP (Captcha gRaphical Password) – TextPoints [38]	×	×	√	×	×	√	×	√	×	√	×	√	×	√	×	√	×	×	×	√	√	○	√	√	√
70	CaRP (Captcha gRaphical Password) – TextPoints4CR (TextPoints for Challenge-Response) [38]	×	○	√	×	×	√	×	√	×	√	×	×	×	√	×	√	×	×	×	√	√	○	√	√	√
Textual-Graphical Hybrid GUA																										
71	Authentigraph [78]	×	○	√	×	×	√	×	√	×	√	×	√	○	×	√	√	×	×	×	×	√	×	√	√	√
72	Cognitive Trapdoor Games [79]	×	×	√	×	×	√	○	√	×	√	×	×	√	×	√	○	√	×	×	×	√	×	√	√	√
73	Screen Oriented Technique [80]	×	○	√	×	×	×	○	√	×	√	×	√	○	×	×	×	×	×	×	×	√	×	√	√	√
74	S3PAS - Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme [81]	×	○	√	×	×	×	○	√	×	√	×	√	○	×	√	○	×	×	×	×	√	×	√	√	√
75	TwoStep [82]	×	○	√	×	○	○	×	√	×	√	×	○	○	×	√	○	×	×	×	×	○	×	√	√	√
76	SS7.0 [83]	×	○	√	×	×	×	×	√	×	√	×	○	○	×	√	×	×	×	×	×	○	×	√	√	√
77	SSSL-Shoulder Surfing Safe Login [84]	×	×	√	×	×	×	×	√	×	√	×	○	○	×	√	×	×	×	×	×	√	×	√	√	√
78	Hybrid Password [85]	×	×	√	×	○	×	×	√	×	√	×	√	×	×	√	×	×	×	×	×	○	○	×	√	√
79	Text-CCP Combination [86]	×	○	√	×	○	×	×	√	×	√	×	○	○	×	√	○	×	×	×	×	×	×	√	√	√
80	Khan's TwoStep [87]	×	○	√	×	○	×	×	√	×	√	×	○	○	×	√	×	×	×	×	×	×	×	√	√	√
81	Pair-Based Authentication Scheme [88]	×	×	√	×	○	×	×	√	×	√	×	○	○	×	√	×	×	×	×	×	×	×	√	√	√
82	Hybrid Textual Authentication Scheme [88]	×	×	√	×	○	×	×	√	×	√	×	○	○	×	√	○	×	×	×	○	×	×	√	√	√
83	Floating-Grid Window Password Scheme [89]	×	×	√	×	○	×	×	√	×	√	×	○	○	×	√	×	×	×	×	×	√	×	√	√	√
84	Advance Secure Login [90]	×	×	√	×	×	×	×	√	×	√	×	○	○	×	√	×	×	×	×	×	×	×	√	√	√
85	Ray's Scheme [91]	×	×	√	×	○	×	×	√	×	√	×	√	×	×	√	×	×	×	×	×	×	×	√	√	√
86	PPC-PairPassChar [92]	×	○	√	×	×	×	×	√	×	√	×	○	○	×	√	×	×	×	×	×	√	×	√	√	√
87	TPPC-TricolorPairPassChar [92]	×	○	√	×	×	×	×	√	×	√	×	○	○	×	√	○	×	×	×	○	×	×	√	√	√
88	T&C-Type & Click [93]	×	×	√	×	○	×	×	√	×	√	×	√	×	×	√	○	×	×	×	○	×	×	√	√	√
89	Text-based shoulder surfing resistant Graphical Password Scheme [94]	×	×	√	×	×	×	×	√	×	√	×	○	○	×	√	○	×	×	×	○	×	×	√	√	√
90	3-Factor Graphical Password [95]	×	√	√	×	×	×	○	×	×	√	×	○	○	×	√	×	×	×	×	×	×	×	√	√	√

Note:

√ Offers the Benefit

○ Almost offers the Benefit

× Does not offer the Benefit

Better than passwords

Worse than passwords

No change

[16] Man, S. , Hong, D. & Mathews, M., "A shoulder-surfing resistant graphical password scheme". Proceedings of International conference on security and management, pp. 1-6, 2003.

[17] Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J.-C., "Design and evaluation of a shoulder-surfing resistant graphical password scheme". Proceedings of the Working Conference on Advanced Visual Interfaces (AVI '06). 177. doi:10.1145/1133265.1133303, 2006.

[18] Hong, D., Man, S., Hawes, B., Mathews, M., "A password scheme strongly resistant to spyware", Proc. International Conference on Security and Management,pp. 94—100, 2004.

[19] Jansen, W., Gavrila, S., Korolev, V., Ayers, R., & Swanstrom, R. , "Picture Password : A Visual Login Technique for Mobile Devices", NISTIR 7030, 2003.

[20] Takada, T., & Koike, H., "Awase-E : Image-based Authentication for Mobile Phones using User's Favorite Images", Human-Computer Interaction with Mobile Devices and Services, Lecture Notes in Computer Science Volume 2795, pp. 347-351, 2003.

[21] Pierce, J. D., Wells, J. G., Warren, M. J., & Mackay, D. R., "A Conceptual Model for Graphical Authentication", 1st Australian Information Security Management Conference. pp.1–8, 2003.

[22] Pering, T., Sundar, M., Light, J., & Want, R., "Photographic authentication through untrusted terminals", IEEE Pervasive Computing, 2(1). 30–36. Doi:10.1109/MPRV.2003.1186723, 2003.

[23] Davis, D., Monrose, F., & Reiter, M. K., "On User Choice in Graphical Password Schemes", 13th USENIX Security Symposium,pp.151-164, 2004.

[24] Tullis, T. S., & Tedesco, D. P., "Using personal photos as pictorial passwords", Extended Abstracts on Human Factors in Computing Systems (CHI '05),pp. 1841-1844. doi:10.1145/1056808.1057036, 2005.

[25] Weinshall, D., "Cognitive Authentication Schemes Safe Against Spyware (Short Paper)", In Proc. IEEE Symposium on Security and Privacy (S&P), pp. 1-6, 2006.

[26] Hinds, C., & Ekwueme, C., "Increasing security and usability of computer systems with graphical passwords", Proceedings of the 45th Annual Southeast Regional Conference on (ACM-SE 45), pp. 529-530, doi:10.1145/1233341.1233448, 2007.

[27] Dunphy, P., & Yan, J. , "Is FacePIN secure and usable?", Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS '07), pp. 165-166, doi:10.1145/1280680.1280710, 2007.

[28] Hayashi, E., Christin, N., Dhamija, R. & Perrig, A., "Use Your Illusion : Secure Authentication Usable Anywhere", Symposium on Usable Privacy and Security (SOUPS 2008), 2008.

[29] Gao, H., Liu, X., Dai, R., Wang, S., & Chang, X., "Analysis and Evaluation of the ColorLogin Graphical Password Scheme", 2009 Fifth International Conference on Image and Graphics, pp.722–727, doi:10.1109/ICIG.2009.62, 2009.

[30] Bicakci, K., Atalay, N. B., Yuceel, M., Gurbaslar, H., & Erdeniz, B., "Towards Usable Solutions to Graphical Password Hotspot Problem", 33rd Annual IEEE International Computer Software and Applications Conference 2009, 318–323. doi:10.1109/COMPSAC.2009.153, 2009.

[31] Gao, H., Liu, X., Wang, S. and Dai, R., "A new graphical password scheme against spyware by using CAPTCHA", Symposium On Usable Privacy and Security (SOUPS) 2009, 2009.

[32] Hasegawa, M., Tanaka, Y., & Kato, S., "A study on an image synthesis method for graphical passwords", 2009 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), pp. 643–646, doi:10.1109/ISPACS.2009.5383758, 2009.

[33] Yamamoto, T., Kojima, Y., & Nishigaki, M., "A shoulder-surfing-resistant image-based authentication system with temporal indirect image selection", 2009 International Conference on Security and Management, pp. 188-194, 2009.

[34] Bashier, H. K., Lau. S.H., & Pang, Y.H., "Graphical password: Pass-images Edge detection", 2013 IEEE 9th International Colloquium on Signal Processing and Its Applications, pp. 111–116, doi:10.1109/CSPA.2013.6530025, 2013.

[35] Van Eekelen, W.,Van den Elst, J. & Khan, V.-J., "Dynamic Layering Graphical Elelments for Graphical Password Schemes", Creating the Difference :Proceeedings of the CHI Sparks 2014, pp. 65-73, 2014.

[36] Liew, T.H., Bashier, H.K., Lau, S.H., Wee, K.K. and Sayeed, M. S., "A Hybrid Graphical Password Scheme for High-End System", Australian Journal of Basic and Applied Sciences,8(2), pp. 23–29, 2014.

[37] Zhu, B., Yan, J., Bao, G., Mao, M., & Xu, N., "Captcha as Graphical Passwords – A New Security Primitive Based on Hard AI Problems", IEEE Transactions on Information Forensics and Security, 6013(c).pp. 1–1, doi:10.1109/TIFS.2014.2312547, 2014.

[38] Rokade, A. H., Hasan, Z. U. & Mahajan, S. A., "User Authentication By Secured Graphical Password Implementation", (IJIRSE) International Journal of Innovative Research in Science & Engineering, 2014.

[39] Blonder, G, "Graphical password". U.S. patent 5,559,961, field August 30, 1995, and issued September 24, 1996

[40] "Sfr", www.sfr-software.de/cms/EN/pocketpc/viskey/index.html, site accessed in Oct, 2012.

[41] Renaud, K. and Smith, E., "Jiminy: Helping user to remember their passwords", Tech. Rep., School of Computing, University of South Africa, 2001.

[42] Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A. & Memon, N., "Authentication Using Graphical Passwords : Effects of Tolerance and Image Choice", Proceedings of the 2005 symposium on Usable privacy and security (SOUPS '05), pp. 1–12, 2005.

[43] Suo, X., "A Design and Analysis of Graphical Password", M.S. thesis, College of Arts and Science, Georgia State University, 2006.

[44] "Passlogix", http://www.passlogix.com, last accessed in Dec 2013.

[45] Yampolskiy, R.V., "User Authentication via Behavior Based Passwords", Systems, Applications and Technology Conference, 2007. LISAT 2007. IEEE Long Island, pp.1-8, 2007.

[46] Lin, P.-L., Weng, L.-T., & Huang, P.-W., "Graphical Passwords Using Images with Random Tracks of Geometric Shapes", 2008 Congress on Image and Signal Processing, pp. 27–31. doi:10.1109/CISP.2008.603, 2008.

[47] Liu, X., Qiu, J., Ma, L., Gao, H., & Ren, Z., "A Novel Cued-recall Graphical Password Scheme", 2011 Sixth International Conference on Image and Graphics, pp. 949–956. doi:10.1109/ICIG.2011.16, 2011.

[48] Lim, K. S., Ithnin, N., & Mammi, H. K., "An Anti-Shoulder Surfing Mechanism and its Memorability Test", International Journal of Security and Its Applications, pp. 87-96, 2012.

[49] Yesseyeva, E., Yesseyev, K., Abdulrazaq, M. M., Lashkari, A. H., & Sadeghi, M., "Tri-Pass : a new graphical user authentication scheme", International Journal Of Circuits, Systems And Signal Processing Volume 8, pp. 61-67, 2014.

[50] Chiasson, S., Oorschot, P. C. Van, & Biddle, R., "Graphical Password Authentication Using Cued Click Points", Computer Security - ESORICS 2007, Lecture Notes in Computer Science Volume 4734, pp. 1–17, 2007.

[51] Stobert, E., Forget, A., Chiasson, S., Oorschot, P. C. Van, & Biddle, R., "Exploring Usability Effects of Increasing Security in Click-based Graphical Passwords", ACSAC'10, pp. 79-88, 2010.

[52] Sun, H.-M., Chen, Y.-H., Fang, C.-C. & Chang S.-Y., "PassMap : A Map Based Graphical-Password Authentication System Categories and Subject Descriptors", ASIACCS '12, pp. 2–6, 2012.

[53] Pandi, M. M. & Valarmathi, A., "A Secured Graphical Password Authentication System", International Journal of Engineering Research & Technology (IJERT), 2(5), pp. 1013–1019, 2013.

[54] Stubblefield, A. & Simon, D. R., "Inkblot Authentication", Technical Report MSR-TR-2004-85, pp. 1–16, 2004.

[55] Syukri, A. F., Okamoto,E. & Mambo, M., "A user identification system using signature written with mouse", Lecture Notes in Computer Science Volume 1438, pp. 403-414, 1998.

[56] Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., & Rubin, A. D., "The Design and Analysis of Graphical Passwords", Proceedings of the 8th USENIX Security Symposium, 1999.

[57] Thorpe, J., & van Oorschot, P. C., "Towards Secure Design Choices for Implementing Graphical Passwords", 20th Annual Computer Security Applications Conference, pp. 50–60. doi:10.1109/CSAC.2004.44, 2004.

[58] Chalkias, K., Alexiadis, A., & Stephanides, G., "A Multi-Grid Graphical Password Scheme", Proceedings of the 6th International Conference on Artificial Intelligence and Digital Communications (AIDC), 2006.

[59] Dunphy, P., & Yan, J., "Do Background Images Improve "Draw a Secret" Graphical Passwords?", Proceedings of the 14th ACM conference on Computer and communications security (CCS '07), pp. 36–47, 2007.

[60] Lin, D., Dunphy, P., Olivier, P., & Yan, J., "Graphical passwords & qualitative spatial relations", Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS '07), pp. 161-162, doi:10.1145/1280680.1280708, 2007.

[61] Chakrabarti, S., Landon, G. V. & Singal, M., "Graphical passwords: drawing a secret with rotation as a new degree of freedom", Proceedings of the Fourth IASTED Asian Conference on Communication Systems and Networks (AsiaCSN '07), pp. 114-120, 2007.

[62] Tao, H., "Pass-Go, a new graphical password scheme", Master's thesis, School of Information Technology and Engineering, University of Ottawa, 2006.

[63] Por, L. Y., Lim, X. T., Su, M. T., & Kianoush, F., "The Design and Implementation of Background Pass-Go Scheme Towards Security Threats", WSEAS Transactions On Information Science & Applications 5(6), pp. 943–952, 2008.

[64] Por, L. Y., & Lim, X. T., "Multi-Grid Background Pass-Go", Wseas Transactions On Information Science & Applications, Issue 7, Volume 5.1137-1148, 2008.

[65] Gao, H., Guo, X., Chen, X., Wang, L., & Liu, X., "YAGP: Yet Another Graphical Password Strategy", 2008 Annual Computer Security Applications Conference (ACSAC), pp. 121–129. doi:10.1109/ACSAC.2008.19, 2008.

[66] Brostoff, S., Inglesant, P., & Sasse, M. A., "Evaluating the usability and security of a graphical one- time PIN system", 24th BCS Conference on Human Computer Interaction (HCI2010), 2010.

[67] Goldberg, J., Hagman, J., & Sazawal, V., "Doodling Our Way to Better Authentication", CHI2002, pp. 868–869, 2002.

[68] Luca, A. De, Weiss, R. & Hussmann, H., "PassShape – Stroke based Shape Passwords", OzCHI 2007, 2007.

[69] Marchetto, J., "pinPass.js:Easy to Use , Easy to Deploy Graphical Passwords", pp. 3–5, n.d.

[70] Li, Z., Sun, Q., Lian, Y., Giusto, D. D., & Star, A., "An Association-Based Graphical Password Design Resistant To Shoulder-Surfing Attack", IEEE International Conference on Multimedia and Expo 2005 (ICME 2005), pp. 2–5, 2005.

[71] Alsulaiman, F. A., & Saddik, A. El., "A Novel 3D Graphical Password Schema", IEEE International Conference on Virtual Environments, Human-Computer Interfaces, and Measurement Systems (VECIMS 2006), pp.10–12, 2006.

[72] Suo, X., "A Design and Analysis of Graphical Password", M.S. thesis, College of Arts and Science, Georgia State University, 2006.

[73] Gao, H., Ren, Z., Chang, X., Liu, X., & Aickelin, U., "A New Graphical Password Scheme Resistant to Shoulder-Surfing", 2010 International Conference on Cyberworlds, pp. 194–199. doi:10.1109/CW.2010.34, 2010.

[74] Éluard, M., Maetz, Y. & Alessio, D., "Action-Based Graphical Password: Click-A-Secret", 2011 IEEE International Conference on Consumer Electronics (ICCE), pp. 265–266, 2011.

[75] Stobert, E., & Biddle, R., "Memory retrieval and graphical passwords", Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13), doi:10.1145/2501604.2501619, 2013.

[76] Haque, A., & Imam, B., "A New Graphical Password : Combination of Recall & Recognition Based Approach", World Academy of Science, Engineering and Technology International Journal of Computer, Information Science and Engineering Vol:8 No:2, pp. 50–54, 2014.

[77] Minne, P., Wells, J., Hutchinson, D., & Pierce, J., "An investigation into the usability of graphical authentication using AuthentiGraph", Proceedings of 5th Australian Information Security Management Conference, pp. 175-186, 2007.

[78] Roth, V., Richter, K., & Freidinger, R., "A PIN-entry method resilient against shoulder surfing", Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS '04), doi:10.1145/1030083.1030116, 2004.

[79] Hoanca, B. & Mock, K., "Screen oriented technique for reducing the incidence of shoulder surfing", Proceedings of International Conference on Security and Management (SAM), 2005.

[80] Zhao, H., & Li, X., "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07). 467–472. doi:10.1109/AINAW.2007.317, 2007.

[81] Oorschot, P. C. Van, & Wan, T., "TwoStep : An Authentication Method", MCETECH 2009, pp. 233–239, 2009.

[82] Mahansaria, D., Shyam, S., Samuel, A., & Teja, R., "A Fast And Secure Software Solution [SS7.0] That Counters Shoulder Surfing Attack", Proceedings of the 13th IASTED International Conference Software Engineering and Applications (SEA2009), pp. 190-195, 2009.

[83] Perkovic, T.; Cagalj, M.; Rakic, N., "SSSL: Shoulder Surfing Safe Login", 17th International Conference on Software, Telecommunications & Computer Networks (SoftCOM 2009), pp. 270-275, 2009.

[84] Zheng, Z., Liu, X., Yin, L., & Liu, Z., "A Hybrid Password Authentication Scheme Based on Shape and Text", Journal of Computers, 5(5). 765–772. doi:10.4304/jcp.5.5, pp. 765-772, 2010.

[85] Singh, C., Singh, L., & Marks, E., "Investigating the Combination of Text and Graphical Passwords for a more secure and usable experience", International Journal of Network Security & Its Applications, 3(2), pp. 78–95. doi:10.5121/ijnsa.2011.3207, 2011.

[86] Khan, W. Z., Aalsalem, M. Y., & Xiang, Y., "A Graphical Password Based System for Small Mobile Devices", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, pp. 145–154, 2011.

[87] Sreelatha, M., Shashi, M., Anirudh, M., Ahamer, M. S., & Manoj Kumar, V., "Authentication Schemes for Session Passwords Using Color and Images", International Journal of Network Security & Its Applications, 3(3), pp. 111–119, doi:10.5121/ijnsa.2011.3308, 2011.

[88] Kim, S.-H., Kim, J.-W., Kim, S.-Y. & Cho, H.-G., "A New Shoulder-Surfing Resistant Password for Mobile Environments", ICUIMC '11, 2011.

[89] Imran, Z., & Nizami, R., "Advance Secure Login", International Journal of Scientific and Research Publications, 1(1), pp. 1–4, 2011.

[90] Ray, P. P., "Ray's Scheme : Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices", Journal of Information Engineering and Applications 2(2), pp. 1–12, 2012.

[91] Rao, M. K., & Yalamanchili, S., "Novel Shoulder-Surfing Resistant Authentication Schemes using Text-Graphical Passwords", International Journal of Information & Network Security (IJINS), 1(3), pp. 163–170, 2012.

[92] Akpulat, M., Bicakci, K., & Cil, U., "Revisiting graphical passwords for augmenting, not replacing, text passwords", Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC '13), pp. 119–128, doi:10.1145/2523649.2523672, 2013.

[93] Chen, Y.-L., Ku, W.-C., Yeh, Y.-C., & Liao, D.-M., "A simple text-based shoulder surfing resistant graphical password scheme", 2013 International Symposium on Next-Generation Electronics, pp. 161–164, doi:10.1109/ISNE.2013.6512317, 2013.

[94] Pohare, J. & Bodade, A., "Graphical password authentication system", International Journal For Engineering Applications and Technology, pp.159-162, 2014.

[95] Bonneau, J., Herley, C., Van Oorschot, P.C. & Stajano, F., "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes", Security and Privacy (SP), 2012 IEEE Symposium on, pp. 553-567, 2012.