Comparative Analysis on Shoulder Surfing Resistant Graphical Password Authentication Systems

Vishvaa Chhatrara chhatraravishvaa@gmail.com
Rutanshi Khambhatiya khambhatiyarutanshi248@gmail.com
Priya Naika priyanaika0612@gmail.com
Harshil Ramanuj dushyantramanuj91@gmail.com

Prof. Naimisha S. Trivedi
Vishwakarma Government Engineering College,
Gujarat, India
naimisha.trivedi@vgecg.ac.in

***Abstract*-The most widely used password authentication technique is the alphanumeric or text password. It has serious drawbacks. To overcome the downsides of these systems, graphical password, secret key validation systems and biometric authentication is introduced. The graphical password strategy could really change how a typical user would insert the password and how secure it could be. It still has its flaws and limitations. One of the limitations of graphical password strategy is that it could be prone to shoulder surfing. Without having a password field just like an alphanumeric password would have, a graphical password can be physically observed especially in public places and an attacker has a clear visual of password being inserted for multiple times, they could easily crack a password which is quite a severe flaw. Another potential limitation of a graphical password strategy is that it is prone to guessing as well. In this paper we will show the drawbacks and limitations of alphanumeric, biometric and graphical password techniques along with graphical password strategies which are proposed to be safe against shoulder surfing**.

Keywords- Graphical Password, Password Authentication, Shoulder Surfing Resistance

I. INTRODUCTION

Authentication is a process of recognizing a user's identity. It is the mechanism of associating an incoming request with a set of identifying credentials. The authentication factors can be defined as: 1. The Knowledge factors: something that a user knows. 2. The ownership factors: something that the user has. 3. The inherence factors: something the user is or does. Knowledge based authentication – alphanumeric password has severe drawbacks such as users tend to pick a small password. It creates difficulty in remembering passwords which are long and hard to break. Text based authentication is prone to vulnerable attacks such as dictionary attack and brute force attack. Besides, the secret key is defenceless against social engineering, shoulder surfing, hidden camera and spyware assaults. To prevent the obstructions of content-based methods, the graphical password has been placed being used. Biometric systems are also vulnerable to its cost, data breaches and inaccuracy. Graphical passwords provide memorability and makes it more challenging to break the system.

II. PURPOSE

The purpose of this report is to provide a brief literature review over shoulder surfing resistant graphical password systems and their methodology, differences, advantages and improvements.

III. BACKGROUND STUDY

A. Authentication:

Authentication is a security measure designed to establish the validity of transmission, message or originator, or a means of verifying an individual's authorization, to receive specific categories of information (NIST.SP.800-59). In simple words, it is the process of validating the identity of a user to provide/allow an access to resources in an information system. The history of password authentication is littered with examples of weak, easily-compromised which are still in use today. The major categories of password authentication systems comprise of weak authentication such as text password, hash password or challenge-response systems. EKE and its modified versions have become to be known as strong encryption and authentication. These can withstand dictionary attacks but they are prone to plain-text equivalency of passwords. OTP and its similar type of authentication systems are inconvenient as they are not entirely password based and require an extra overhead on the part of users and administrators to operate smoothly. (History of Authentication) Among the factors of the authentication process, that are, knowledge factors, possession factors and biometric factors, knowledge factors in the form of text passwords are commonly used.

B. Text/PIN Passwords:

Text based password authentication is a traditional way of proving one's identity during registration and login phase. Text passwords are the combination of alphabets, numbers and some special symbols. The user needs to memorize the password to enter the system. The memorization of passwords is a critical issue nowadays, there are more than a billion websites and applications that use text passwords and a common user deals with at least 10-15 applications on average in a day. For a normal human being, it is difficult to remember all passwords and if the chosen password would be too small or simple to remember then, the account of that user can be easily broken using dictionary / brute force / guessing or any other equivalent attacks. These attacks can be reduced by limiting the number of attempts and by locking the account temporarily. Sometimes, users use the same password for

different services, this may put the user at risk of getting hacked if the password of any one of its applications is known by the hacker.

C. *Graphical Passwords:*

Graphical password systems are proposed as advancement to the alphanumeric password which will overcome the drawbacks of textual password. Some psychological and scientific studies have proven that pictures and visuals are easier to remember than texts. Also, the pictures which are used in graphical passwords have thousands of pixel points whose values can be used as a part of password string. [3] Graphical password system can be divided into 3 categories: Recognition based, Recall based and Cued recall based. [2]

a) *Recognition based authentication*: A user is given a set of images and he has to identify the image he selected during registration. For example, Passfaces is a graphical password scheme based on recognizing human faces. During password creation, users are given a large set of images to select from. A log-in user has to identify the pre-selected images from the several images presented to him.

b) Recall based authentication: A user is asked to reproduce something that he had created or selected at the registration phase. For example, in the Passpoint scheme, a user can click on any point in an image to create a password and a tolerance around each pixel is calculated. During authentication, the user has to select the points within the tolerance in the correct sequence to login.

c) Cued Recall based authentication: Cued click points (CCP) is an alternative to passpoint scheme. In CCP, users click on points on each image rather than 5 points on one image (unlike Passpoints). It offers cued recall and instantly alerts the user if they make a mistake while entering their latest click-point.

IV. SECURITY AND ATTACKS

Passwords are there to provide assurance that the user entering the system is authenticated and thus password is a kind of security measure. But textual passwords are themselves vulnerable to Brute force search, keylogger attack, dictionary and guessing attacks. Graphical passwords are resistant to these kinds of attacks but they are still prone to shoulder surfing and social engineering attacks. However, an equivalent of dictionary attack could be to analyse a certain system to figure out which icons or patterns are more attractive to users. The points of the images which are more clicked by the user rather than clicking on random other points, creates a hotspot. These hot spots can be easily detected by attackers. Graphical passwords can be designed in such a way that it makes it difficult for attackers to figure out the password.

V. USABILITY, DESIGN AND TESTING

Usability refers to the quality of the user's experience while interacting with the product or system. It is about efficiency, effectiveness and overall satisfaction of user. (Usability) Usability of a password system refers to how easy it is for the right person to authenticate. Reason behind weak password usability and security in textual passwords is because of the difficulty in creating secure password and remembering it. (Password security and usability) Most studies on security shows that frameworks can either be secure or usable, not both. There is some literature that recommends that considering usability prior to security may provide the best possible setup. PC security exploration and Convenience are the two standards into different password validation arrangements. Passphrases and Two factor authentication provide good usability but poor implementation. Implementation refers to the design of the system and how easy it is to set up and support. 2FA-like systems eat the time of the user to login and because of it, people don't prefer to use it. But it provides the benefit that it doesn't rely completely on password.

The goal of any software design is the simplicity in access and navigation. Design implementation of any graphical password system would refer to Input design (i.e., Input to the front end of the system is designed to be the graphical password, user photos are used instead of typing a password.) and Control design (i.e., control provides ways to: registration is mandatory before login.)

The graphical password authentication systems are tested based on some human factors by studying two issues: the effect of tolerance, the margin of error, in clicking in the password points and the effect of the image used in the password systems. Small tolerance around pixel provides a strong password but user may fail to precisely encode the password in the memory. (Effect of tolerance and image choice)

VI. THEORETICAL CONCEPTS

A. *Password Space:*

The number of possible combinations that exist for a password is called password space. Generally, the larger password space a system has, the safer it is against guessing attacks. The password space in a system (S) depends on the total number of symbols available (T) and the number of symbols in the password (p). This can be compared to the password space of graphical password which depends on the total number of icons or the library in the positions in the picture (T) and the number of icons or click-points in the password (p).

$$S = T^p$$

The theoretical password space in graphical password assumes an equiprobable distribution of passwords. Its size corresponds to the theoretical computational effort of an adversary guessing the password with exhaustive search over all potential passwords (brute force). For the graphical passwords, the "character set" is defined by the employed visual elements and a password is specified. The password length corresponds to the length of recognition or recall sequence. [4]

The practical password space in graphical passwords is defined as the probability of an adversary guessing the password based on the statistical distributions of a password for the given scheme. For many schemes, optimizations have been proposed as design features to influence user choice towards flatter and less predictable password distributions. [4]

B. *Shoulder Surfing:*

Observation attacks aka Shoulder surfing is considered a major threat aimed to obtain a user's password through observation of login process. Most often, the concerns

regarding shoulder surfing attacks are addressed in papers introducing novel graphical password authentication methods. Resistance against shoulder surfing attacks has become an expectation particularly for graphical passwords which are more susceptible to them. Some research papers, these days, propose a shoulder surfing method but they have not tested the system beyond theoretical level and some identify the investigation of the method's resistance as a plausible direction for future research. [5]

A paper published in October 2019 named – *Shoulder surfing: from an experimental study to a comparative framework* has shown a comparative framework that allows for an in-depth analysis of shoulder surfing. From the reference of this paper [5] along with 2 other papers ([1], [2]), we have summarized different shoulder surfing resistant techniques as follows.

VII. LITERATURE REVIEW OF DIFFERENT SHOULDER SURFING RESISTANT TECHNIQUES

1. *Sun et al. – Passmatrix – 2018*

In this method, the user chooses points in a sequence of images which he or she will have to remember. The system is based on cued-recall based systems. During authentication, the user uses a key consisting of a letter and a number which have to be aligned with the previously selected points on the images using scroll bars on the X and Y axis. A key is gathered by placing a hand around the part of the screen in such a way that only the user can see the key (see Fig 1).

Another way to get the key is to listen to it through speakers or headphones. The user applies the same key to three to five images depending on how many the user specified in registration. The key is randomly generated with every authentication attempt.

Figure 1. Sun et al. Passmatrix

Characteristics: a) Easy to remember, b) Shoulder surfing resistant, c) Interaction method: android devices, d) Constraints: can be used on mobile devices.

2. *Wu et al. – Convex hull graphical algorithm and dynamic objects*

In this method, the convex hull algorithm is applied where the user is required to remember some icons from the library while registering. And while login, the user has to click anywhere within the triangle convex hull region marked by the placement of pass-icons instead of having to click on an actual pass-icon. (Fig 2)

Wu et al. also added extra space to password as clicking on the pre-selected and randomly moving coloured balls and pressing the preselected key of keyboard. Password space was then increased to 2^{34}. [2]

Figure 2. Wu et al. convex hull graphical algorithm

Characteristics: a) Shoulder surfing resistant, b) Large password space, c) Spyware and guessing attack resistant, d) Higher memory burden when increased security (less memorability or more login time / practice required), e) A small price to pay to make password more secure.

3. *Roth et at. – PIN entry method [2]*

PIN is the personal identification number. On the display screen, all the numbers are represented in randomly black or white color and randomly placed on a screen. Refer to Fig 3 User need to select the color sequence of the PIN digits. The system resists the direct shoulder surfing but it is prone to hidden video or camera recording. [5]

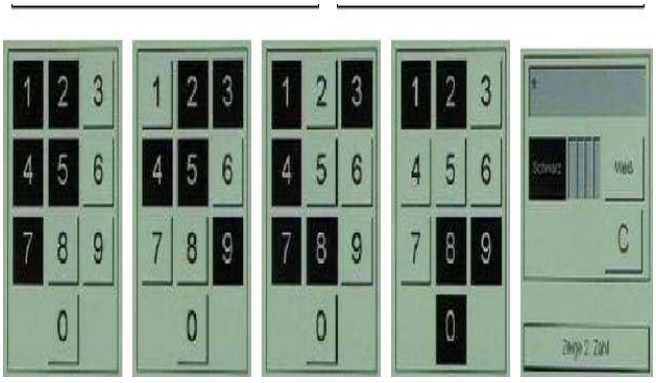

Figure 3. Roth et al. PIN Entry method

Characteristics: a) Less password space, b) Usability: moderate in case of regular system, c) Prone to hidden camera and recording

4. *FakePointer – T. Takada*

This technique was developed to prevent video shoulder surfing. It provides two features. First is a double layered user interface for a secret input. And fake pointer is the second feature. (Fig 4) This method has a huge password lifespan and easy password recall. But password length is long. [6]

Figure 4. FakePointer T. Takada

Characteristics: a) Less shoulder surfing resistant, b) Good memorability, c) Pointers used

5. *Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS)*

This system integrates both graphical and textual password scheme. It can replace or coexist with conventional textual password systems without changing existing user profiles. It uses session passwords so that it is prone to brute force attack. It is similar to the convex hull system where the user has to click inside the region formed by the 3 consequent letters following a certain click rule. And after each click, the position of the characters on the login screen is changed. (Fig 5) [7]

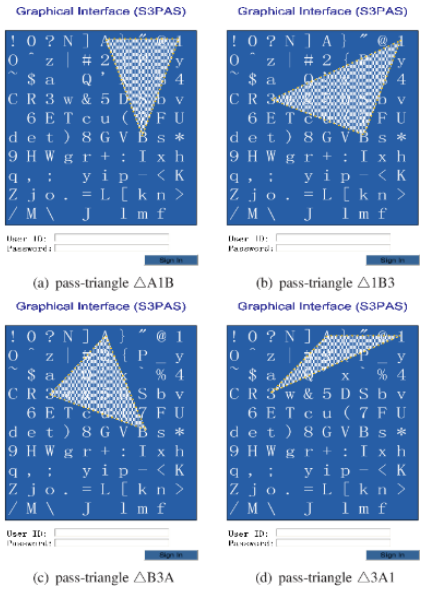

Figure 5. S3PAS

Characteristics: a) Shoulder surfing resistant, b) Better security when area of the triangle formed is less, c) Brute force search resistant, d) Memorability is same as the textual password scheme, e) More login time required

6. *Chiasson et al. - Cued Click Points*

In this technique, more than one image as a sequence is used as a password. User click on one point per image for a sequence of images. The next image is based on the previous click point. It is the more advanced technique to the Pass-point scheme proposed by Weidenbach et al. [10] where the user was required on the multiple points in the same image. [8] Refer to Fig 6.

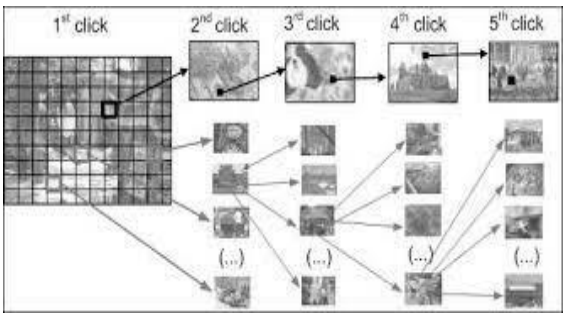

Figure 6. Chaisson et al. Cued Click Points

Characteristics: a) Good performance in speed, accuracy and number of errors. b) Increased memorability, c) More time required in password creation, less in login and confirmation, d) Prone to video capturing based attacks, e) Prone to hotspot attacks, f) Good performance and increased usability

7. *Weinshall – machine generated pictures*

A bunch of machine-generated images are used by the user as a password. The user has to remember those pictures. While login, the user has to recall the path with password images and answer a multiple-choice question. The series of such challenges result in authentication. The software will verify the path. Because the path is known only by the user and system, no other shoulder surfer or camera can trace the path. [9]

Characteristics: a) More login time required, b) Shoulder surfing resistant, c) Increased memorability after training, d) More computer memory consumed because of large number of images

8. *Tan et al. – spy resistant keyboard*

The approach for designing this system is security-sensitive onscreen virtual keyboards where users can enter private text without revealing it to observers. This approach adds ambiguity for the watcher such that it is unable to determine the user's choice. The shoulder surfer has to remember the layout of the keyboard to guess the password. [11]

Figure 7. Tan et al. Spy Resistant Keyboard

Characteristics: a) More login time required, b) Complex interaction technique, c) Increase in shoulder surfing resistance

9. *Meader et al. – gaze-based password*

This approach is based on the gaze sequence of the observer when presented with a previously seen image on screen. The user keeps the eye without motion for few micro seconds on a point while focusing on it. The camera or an eye tracker fixed in it will track the movement of the eyes and capture the locations where the eye stops. These passwords can be textual or graphical and the password length can be kept the same but unobservable by the shoulder surfing person or camera. [12]

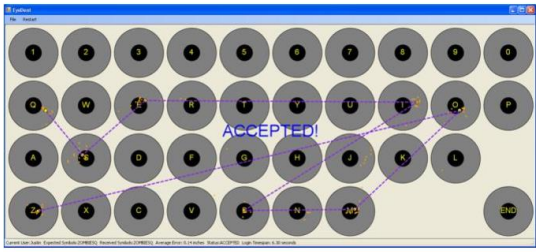

Figure 3. Alphanumeric keyboard layout showing a successful login attempt for the password "ZOMBIESQ".

Figure 8. Meader et al. Gaze based password

10. *Thorpe et al.- Pass-Thoughts*

The similar to above approach named pass-thoughts which is based on the gaze-based typing was presented by Thorpe et al. in [13]. It proposes that the user will think of a password in his mind and that thought will be then transmitted to a computer. So it focuses on the human computer interaction without using gestures.

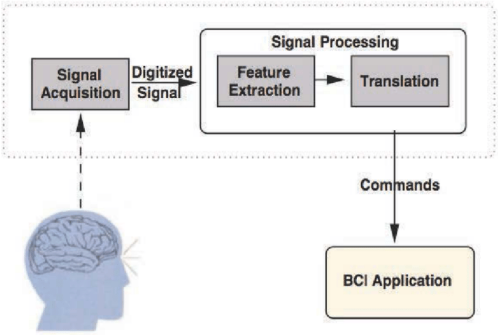

Figure 9. Thrope et al. Pass Thoughts

Characteristics: a) Shoulder surfing resistant, b) Prone to social engineering attack, c) Other security concerns are similar to textual password as password is textual.

11. *Yu et al. – EvoPass*

EvoPass is the evolvable graphical password authentication system. Here the pass images are first transformed into pass sketches and users have to choose the correct pass sketches. EvoPass degrades the pass sketch continually without creating any trouble for users to reselect pass images and thus, it improves the password strength gradually. It becomes difficult for shoulder surfers to observe the partially transformed pass sketches. [14]

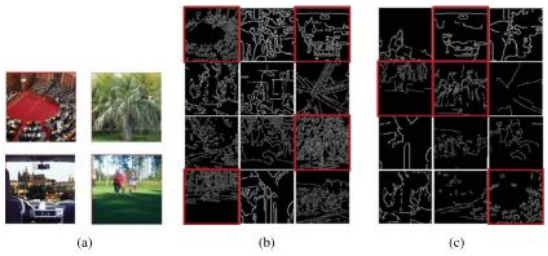

Figure 10. Yu et al. EvoPass

Characteristics: a) Improves shoulder surfing resistance gradually, b) No impact on user experience., c) Experienced users get better usability and interaction with the system.

12. *Papadopoulos et al.*

IllusionPIN - Shoulder surfing resistant authentication using Hybrid Images is a PIN based authentication which works on the android or mobile touch screen devices. This method creates an illusion to the attacker such that the keyboard that an attacker watches is different from the original that the person is near to the device and entering the PIN. It hybrids two keypads and shuffles the digits of the keypad every login time. It is based on Human Visual Perception algorithm. [15]

Figure 11. Papadopoulos et al. IllusionPIN

Characteristics: a) Shoulder surfing resistant, b) Dependant on measures of safety distance, c) Visibility parameters should be appropriately set

13. *Maqsood et al. - Bend passwords*

This scheme uses bend gestures for the smart mobile devices as its input modality. Users interact with the device by deforming / bending the surface of the device. Such flexible display devices can be applied to gaming, control of media and home appliances, maps and smartphones.

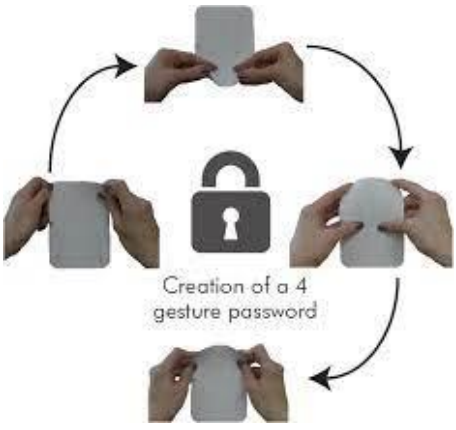

Figure 12. Maqsood et al. Bend Passwords

Characteristics: a) Authentication mechanism for flexible display devices, b) Better memorability, c) Easier to operate, d) Higher login time, e) Secure against shoulder surfing.

VIII. MEASURES THAT ARE USED TO TEST DESIGN, CHARACTERISTICS AND CAPABILITIES

a) *Security*: How secure the system is against brute force, guessing, spyware and other attacks.
b) *Observed Resistance*: It checks whether the system is less vulnerable against hidden camera and video recording observation attacks or not.
c) *Efficiency*: How much login time is required by a normal user. Whether it is too much or reasonable.
d) *Memorability:* How easy is password to be remembered by the user. Whether the users can recall the password quickly or how much time it takes to remember and recollect the password.
e) *Spatial Arrangement:* This design feature says that how the objects on the screen are arranged, whether they are randomized or fixed by position.
f) *Temporal Arrangements:* In this measure we ensure that whether every time login screen of the user is changed or how many challenges it provides with fixed or changing backgrounds.
g) *Visual Cues:* These simply are the size or the dimensions of the visual elements. Whether they are large/small and the amount of detail it provides.
h) *Interaction method:* The interaction method of any password system enlists whether the user interacts with the system using keyboard or mouse or touchscreen or any other data input tool.
i) *Context of use:* It is the probability of any user/attacker to guess or remember the password after certain attempts or certain number of observations.
j) *Constraints:* It asks the system whether it can be useful for any visually or physically challenged user.

IX. KEY PROBLEMS

a) Most widely used technique is textual password where people tend to use plain or simple text as password and which can be easily guessed. Again, too strong textual password is difficult to guess but difficult to remember and recollect.
b) Additional intricacy is added into the system while making it shoulder surfing resistant
c) Shoulder surfing is an issue that has been hard to overcome
d) Ease of use, memorability, security, difficulty in recollecting
e) Textual watchwords are helpless against shoulder surfing, shrouded camera and spyware assaults. Graphical passwords are helpless against shoulder surfing too.
f) Individual scheme investigations and diverse measures
g) Susceptibility to shoulder surfing was measured using simple techniques, such as proportion of the password being guessed correctly

X. CONCLUSION

In this paper we studied some well-known shoulder surfing resistant graphical password authentication schemes. We can conclude that the Shoulder Surfing unprotected ness does not only depend upon the type of password whether it is graphical or textual but also depends upon the overall design and architecture of the system. Every graphical password system has their own pros and cons. Each of them satisfies some criteria of security and usability but none of them can assure complete security. The improved and updated versions of some systems are giving better protection and we can further improve the existing ones or can develop new techniques which may be the hybrid of all of them such that it covers most of the requirements.

In future work with these technologies, we look forward to introducing the combination of graphical password with biometric systems. In this way, we can overcome the drawbacks of graphical password authentication and add more strength to the system to stand against shoulder surfing, social engineering and similar types of attacks.

REFERENCES

[1] Dhanashree Chaudhari, "A Survey on Shoulder Surfing Resistant Text Based Graphical Password Schemes", International Journal of Science and Research (IJSR), https://www.ijsr.net/search_index_results_paperid.php?id=NOV151759, Volume 4 Issue 11, November 2015, 2418 – 2422

[2] Alesand, E., & Sterneling, H. (2017). A shoulder-surfing resistant graphical password system.

[3] D. Gupta, A. P. Singh, V. Goar and S. Mathur, "Combination of textual and graphical based authentication scheme through virtual environment," 2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall), Dehradun, India, 2017, pp. 1-4, doi: 10.1109/ICACCAF.2017.8344705.

[4] https://cups.cs.cmu.edu/soups/2013/proceedings/a11_Schaub.pdf

[5] Leon Bošnjak, Boštjan Brumen, Shoulder surfing: From an experimental study to a comparative framework, International Journal of Human-Computer Studies, (https://www.sciencedirect.com/science/article/pii/S1071581918305366)

[6] Alese, B. K., Omojowo, A. A., Adesuyi, A. T., Thompson, A. F., Adewale O. S., & Osuolale F. O. (2015). An Enhanced Graphical Password Technique Using Fake Pointers. Proceedings of Informing Science & IT Education Conference (InSITE) 2015, 79-89. Retrieved from http://Proceedings.InformingScience.org/InSITE2015/InSITE15p079-089Alese1551.pdf

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

[8] Chiasson S., van Oorschot P.C., Biddle R. (2007) Graphical Password Authentication Using Cued Click Points. In: Biskup J., López J. (eds) Computer Security – ESORICS 2007. ESORICS 2007. Lecture Notes in Computer Science, vol 4734. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74835-9_24

[9] Weinshall, Daphna & Kirkpatrick, Scott. (2004). Passwords You'll Never Forget, But Can't Recall. Proc. CHI 2004. 10.1145/985921.986074. https://www.cs.huji.ac.il/~kirk/Imprint_CHI04_final.pdf

[10] Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget. 2006. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In Proceedings of the working conference on Advanced visual interfaces (AVI '06). Association for Computing Machinery, New York, NY, USA, 177–184. DOI:https://doi.org/10.1145/1133265.1133303

[11] Tan, D. S., P. Keyani, and M. Czerwinski. Spy-Resistant Keyboard: Towards More Secure Password Entry on Publicly Observable Touch Screens. In Proceedings of OZCHI - Computer-Human Interaction Special Interest Group (CHISIG) of Australia. Canberra, Australia: ACM Press, 2005

[12] A. Maeder, C. Fookes and S. Sridharan, "Gaze based user authentication for personal computer applications," Proceedings of 2004 International Symposium on Intelligent Multimedia, Video and Speech Processing, 2004., Hong Kong, China, 2004, pp. 727-730, doi: 10.1109/ISIMP.2004.1434167.

[13] Thorpe, Julie & Oorschot, Paul & Somayaji, Anil. (2005). Pass-thoughts: Authenticating With Our Minds.. IACR Cryptology ePrint Archive. 2005. 121. 10.1145/1146269.1146282. https://eprint.iacr.org/2005/121.pdf

[14] Yu, Xingjie & Wang, Zhan & Li, Yingjiu & Li, Liang & Zhu, Wen & Song, Li. (2017). EvoPass: Evolvable graphical password against

shoulder-surfing attacks. Computers & Security. 70. 10.1016/j.cose.2017.05.006.

[15] Papadopoulos, Athanasios & Nguyen, Toan & Durmus, Emre & Memon, Nasir. (2017). IllusionPIN: Shoulder-Surfing Resistant Authentication Using Hybrid Images. IEEE Transactions on Information Forensics and Security. PP. 1-1. 10.1109/TIFS.2017.2725199.

[16] Sana Maqsood, Sonia Chiasson, and Audrey Girouard. 2016. Bend Passwords: using gestures to authenticate on flexible devices. Personal Ubiquitous Comput. 20, 4 (August 2016), 573–600. DOI:https://doi.org/10.1007/s00779-016-0928-6