Trends in Engineering and Technology (NCTET-2K17)
International Journal of Advanced Engineering Research and Science (IJAERS) *Special Issue-3*
https://dx.doi.org/10.22161/ijaers/nctet.2017.13 *ISSN: 2349-6495(P) | 2456-1908(O)*

A Novel Authentication System Passmatrix Based On Graphical Passwords

M.Sravanasree[1], T.Satyendra Kumar[2]

[1]PG Scholar, Department of CSE, S.V.E.W, sravanasri@gmail.com
[2]Assistant Professor, Department of CSE, S.V. E.W,satya.thallapaka@gmail.com

ABSTRACT:-- Authentication in view of passwords is utilized to a great extent in applications for PC security and protection. Nonetheless, human activities, for example, picking awful passwords and contributing passwords in an unreliable way are viewed as "the weakest connection" in the validation chain. As opposed to subjective alphanumeric strings, clients have a tendency to pick passwords either short or important for simple remembrance. With web applications and versatile applications heaping up, individuals can get to these applications at whatever time and anyplace with different gadgets. This advancement brings awesome accommodation additionally builds the likelihood of presenting passwords to shoulder surfing assaults. Assailants can watch specifically or utilize outer recording gadgets to gather clients' accreditations. To defeat this issue, we proposed a novel confirmation framework PassMatrix, in view of graphical passwords to oppose bear surfing assaults. With a one-time legitimate login pointer and circulative even and vertical bars covering the whole extent of pass-pictures, PassMatrix offers no insight for assailants to make sense of or limit the secret key even they lead various camera-based assaults. We additionally executed a PassMatrix model on Android and done genuine client examinations to assess its memorability and convenience. From the trial result, the proposed framework accomplishes better imperviousness to shoulder surfing assaults while looking after ease of use.

Index Terms—Graphical Passwords, Authentication, Shoulder Surfing Attack.

1. INTRODUCTION

Printed passwords have been the most by and large used approval procedure for a significant time allotment. Included numbers and upper-and lower-case letters, abstract passwords are seen as adequately strong to restrict against brute force attacks. Regardless, a strong scholarly watchword is hard to recollect and review. Accordingly, customers tend to pick passwords that are either short or from the dictionary, rather than self-assertive alphanumeric strings. By a long shot more loathsome, it is not an extraordinary case that customers may use only a solitary username and mystery word for different records. As shown by an article in Computer world, a security gather at a colossal association ran a framework mystery word

saltine and shockingly broke around 80% of the delegates' passwords inside 30 seconds. Printed passwords are every now and again indeterminate as a result of the inconvenience of keeping up strong ones. Diverse graphical watchword approval arrangements were made to address the issues and deficiencies related with printed passwords. In light of a couple audits, for instance, those in individuals have a better limit than hold pictures with whole deal memory (LTM) than verbal depictions. Picture based passwords were ended up being less requesting to recall in a couple customer analyzes. Thusly, customers can set up a puzzling approval watchword and are prepared for recollecting that it after a long time paying little respect to the likelihood that the memory is not established discontinuously. Regardless, by far most of these photo based passwords are exposed against shoulder surfing strikes (SSAs). This kind of strike either uses organize observation, for instance, seeing behind somebody or applies video getting methodology to get passwords, PINs, or other sensitive individual information. The human exercises, for instance, picking dreadful passwords for new records and contributing passwords in a temperamental way for later logins are seen as the weakest association in the confirmation chain. In this way, an approval arrange should be expected to vanquish these vulnerabilities. In this paper, we show a safe graphical approval system named PassMatrix that shields customers from getting the opportunity to be losses of shoulder surfing ambushes while contributing passwords out in the open through the usage of one-time login markers. A login marker is self-assertively delivered for each pass-picture and will be pointless after the session closes. The login marker

https://dx.doi.org/10.22161/ijaers/nctet.2017.13 *ISSN: 2349-6495(P) | 2456-1908(O)*

gives better security against shoulder surfing strikes, since customers use a dynamic pointer to point out the position of their passwords as opposed to tapping on the mystery key challenge particularly.

As the convenient publicizing bits of knowledge aggregation by Danyl, the flexible shipments had outperformed PC shipments in 2011, and the amount of adaptable customers also overpowered desktop customers at 2014, which closed to 2 billion. In any case, bear surfing ambushes have spoken to a mind boggling danger to customers' security and mystery as phones are getting the opportunity to be doubtlessly vital in current life. People may sign into web organizations and applications out in the open to get to their own particular records with their propelled cell phones, tablets or open contraptions, like bank ATM. Bear surfing aggressors can observe how the passwords were entered with the help of reflecting glass windows, or also screens hanging wherever out in the open spots. Passwords are exhibited to perilous circumstances, paying little mind to the likelihood that the passwords themselves are brain boggling and secure. An ensured approval structure should have the ability to shield against shoulder surfing ambushes and should be fitting to an extensive variety of devices. Approval contrives in the written work, for instance, those in are impenetrable to shoulder-surfing, be that as it may they have either comfort obstructions or minimal mystery word space. Some of them are not sensible to be associated in phones and by far most of them can be successfully exchanged off to shoulder surfing strikes if aggressors use video getting techniques like Google Glass. The requirements of comfort consolidate issues, for instance, putting aside more noteworthy chance to sign in, passwords being too much troublesome, making it difficult to survey after a time span, and the confirmation system being exorbitantly frustrated for customers without proper direction and practice.

In 2006, Wiedenbeck et al. proposed PassPoints in which the customer gets a couple centers (3 to 5) in a photo in the midst of the mystery word creation stage and re-enters each of these pre-picked click-centers in a correct demand inside its tolerant square in the midst of the login organize. Standing out from standard PIN and abstract passwords, the Pass-Points contrive fundamentally extends the watchword space and enhances mystery word memorability. Tragically, this graphical approval plan is feeble against shoulder surfing attacks. From this time forward, in perspective of the PassPoints, we incorporate using one-time session passwords and distracters to develop our PassMatrix approval system that is impenetrable to shoulder surfing strikes.

2. RELATED WORK

In the previous quite a few years, a great deal of research on secret key confirmation has been done in the writing. Among these proposed plans, this paper concentrates for the most part on the graphical-based validation frameworks. To keep this paper compact, we will give a concise survey of the most related plans that were specified in the past area. Numerous different plans, for example, those in [27], [28], [29], [30], [31] may have great convenience, they are not graphical-based and require extra support from additional equipment, for example, sound, multi-touch screen, vibration sensor, or gyrator, and so forth. In the good 'ol days, the graphical capacity of handheld gadgets was powerless; the shading and pixel it could show was constrained. Under this constraint, the Draw-a-Secret (DAS) [6] system was proposed by Jermyn et al. in 1999, where the client is required to re-draw a pre-characterized picture on a 2D framework. We specifically extricate the figure from [6] and show it in Figure 1(b). In the event that the drawing touches similar frameworks in a similar arrangement, at that point the client is confirmed. From that point forward, the graphical ability of handheld gadgets has relentlessly and endlessly enhanced with the advances in science and innovation. In 2005, Susan Wiedenbeck et al. presented a graphical confirmation conspire PassPoints [7], and around then, handheld gadgets could as of now show high determination shading pictures. Utilizing the PassPoint plot, the client needs to tap on an arrangement of pre-characterized pixels on the fated photograph, as appeared in Figure 1(a) (this figure is separated from [7]), with a right grouping and inside their tolerant squares amid the login organize. Additionally, Marcos et al. likewise expanded the DAS in view of finger-drawn doodles and pseudosignatures in late cell phone [32], [33]. This validation framework depends on components which are separated from the elements of the motion drawing process (e.g., speed or increasing speed). These components contain behavioral biometric trademark. At the end of the day, the assailant would need to impersonate what the client draws, as well as how the client draws it. Be that as it may, these three confirmation plans are still all defenseless against shoulder surfing assaults as they may uncover the graphical passwords specifically to some obscure eyewitnesses openly. Notwithstanding graphical validation plans, there was some examination on the augmentation of customary individual recognizable proof number (PIN) section confirmation frameworks. In 2004, Roth et al. [34] exhibited an approach for PIN passage against shoulder surfing assaults by expanding the clamor to eyewitnesses. In their approach, the PIN digits are shown in either dark or white haphazardly in each round. The client must react to the framework by recognizing the shading for every secret word digit. After the client has settled on a progression of parallel options (dark or

https://dx.doi.org/10.22161/ijaers/nctet.2017.13 *ISSN: 2349-6495(P) | 2456-1908(O)*

white), the framework can make sense of the PIN number the client planned to enter by converging the client's decisions. This approach could befuddle the spectators on the off chance that they simply watch the screen with no assistance of video catching gadgets. Be that as it may, if spectators can catch the entire verification prepare, the passwords can be broken effectively. Keeping in mind the end goal to safeguard the shoulder surfing assaults with video catching, FakePointer [35] was presented in 2008 by T. Takada. We utilize Figure 2 (from [35]) underneath to demonstrate the use of FakePointer. Notwithstanding the PIN number, the client will get another "answer pointer" each time for the validation procedure at a bank ATM. As it were, the client has two mysteries for validation: a PIN as a settled mystery and an answer marker as a dispensable mystery. The appropriate response pointer is an arrangement of n shapes if the PIN has n digits. At each login session, the FakePointer interface will exhibit the client a picture of a numeric keypad with 10 numbers (like the numeric keypad for telephones), with each key (number) on top of an arbitrarily picked shape. The numeric keys, however not the shapes, can be moved circularly utilizing the left or right bolt keys. Amid confirmation, the client should more than once move numeric keys circularly as appeared in the furthest left figure in Figure 2, until the main digit of the PIN covers the principal state of the appropriate response pointer on the keypad and afterward affirm a determination by squeezing the space key. This operation is rehashed until all the PIN digits are entered and affirmed. This approach is very vigorous notwithstanding when the assailant catches the entire verification handle. Be that as it may, there is still space to enhance the secret word space. For instance, if the gadget utilized for confirmation is a cell phone, a tablet or a PC instead of a bank ATM, the secret word space can be developed significantly since the PIN could be any blend of alphanumeric characters as opposed to simply numeric digits.

3. EXISTING SYSTEM

•Wiedenbeck et al. proposed PassPoints in which the client gets a few focuses (3 to 5) in a picture amid the secret key creation stage and re-enters each of these pre-chosen click-focuses in a right request inside its tolerant square amid the login stage. Contrasting with customary PIN and literary passwords, the Pass-Points plot significantly builds the secret key space and improves watchword memorability.

•David Kim et al. proposed a visual confirmation plot for tabletop interfaces called "Shading Rings", where the client is alloted i validation (key) symbols, which are by and large allocated one of the four shading rings: red, green, blue, or pink.

DISADVANTAGES OF EXISTING SYSTEM

- • Most of the current framework picture based passwords are helpless against shoulder surfing assaults (SSAs). This sort of assault either utilizes coordinate perception, for example, viewing behind someone or applies video catching procedures to get passwords, PINs, or other touchy individual data
-
- • Some of them are not appropriate to be connected in cell phones and the greater part of them can be effectively traded off to shoulder surfing assaults if aggressors utilize video catching methods like Google Glass.
-
- • The constraints of ease of use incorporate issues, for example, setting aside greater opportunity to sign in, passwords being excessively troublesome, making it impossible to review after a timeframe, and the verification strategy being excessively muddled for clients without appropriate instruction and practice.If observers are able to capture the whole authentication process, the passwords can be cracked easily.
- A large number of objects will crowd the display and may make objects indistinguishable.
- These kinds of passwords can be cracked by intersecting the user's selections in each login because the color of the assigned ring is fixed and a ring can include at most seven icons. Thus, the attacker only requires a limited number of trials to guess the user's password.

4. PROPOSED SYSTEM:

• In this paper, we display a safe graphical verification framework named PassMatrix that shields clients from getting to be casualties of shoulder surfing assaults while contributing passwords out in the open through the use of one-time login markers.

• A login marker is haphazardly produced for each pass-picture and will be futile after the session ends. The login marker gives better security against shoulder surfing assaults, since clients utilize a dynamic pointer to call attention to the position of their passwords instead of tapping on the secret key protest straightforwardly.

https://dx.doi.org/10.22161/ijaers/nctet.2017.13 *ISSN: 2349-6495(P) | 2456-1908(O)*

• The existing graphical confirmation plan is powerless against shoulder surfing assaults. Consequently, in view of the PassPoints, we include utilizing one-time session passwords and distracters to build up our PassMatrix validation framework that is impervious to shoulder surfing assaults.

ADVANTAGES OF PROPOSED SYSTEM:

- The passwords of our PassMatrix are easy to memorize.
- Users can log into the system with only 1:64 (Median=1) authentication requests on average, and the Total Accuracy of all login trials is 93:33% even after two weeks.
- Passwords are not exposed to risky environments.
- The proposed system acts as a secure authentication system and will be able to defend against shoulder surfing attacks and will be applicable to all kinds of devices.

5. SYSTEM ARCHITECTURE

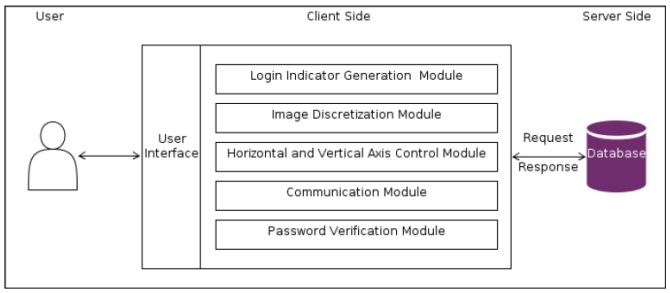

Figure:1 System Architecture

Shoulder Surfing Attacks

Based on previous research users' actions such as typing from their keyboard, or clicking on the pass-images or pass-points in public may reveal their passwords to people with bad intention. In this paper, based on the means the attackers use, we categorize shoulder surfing attacks into three types as below:

1) Type-I: Naked eyes.
2) Type-II: Video captures the entire authentication process only once.
3) Type-III: Video captures the entire authentication process more than once.

The latter types of attacks require more effort and techniques from attackers. Thus, if an authentication scheme is able to resist against these attacks, it is also secure against previous types of attacks. Some of the proposed authentication schemes including traditional text-password and PIN, are vulnerable to shoulder surfing

Type-I attacks and thus are also subject to Type-II and Type- III attacks. These schemes reveal passwords to attackers as soon as users enter their passwords by directly pressing or clicking on specific items on the screen. Other schemes such as those in can resist against Type-I but are vulnerable to Type-II and Type-III attacks since the attackers can crack passwords by intersecting their video captures from multiple steps of the entire authentication process.

Smudge Attacks

According to a previous study authentication schemes that require users to touch or fling on computer monitors or display screens during the login phase are vulnerable to smudge attacks. The attacker can obtain the user's password easily by observing the smudge left on the touch screen

PASSMATRIX

• In this paper, we display a safe graphical verification framework named PassMatrix that shields clients from getting to be casualties of shoulder surfing assaults while contributing passwords out in the open through the use of one-time login markers.

• A login marker is haphazardly produced for each pass-picture and will be futile after the session ends. The login marker gives better security against shoulder surfing assaults, since clients utilize a dynamic pointer to call attention to the position of their passwords instead of tapping on the secret key protest straightforwardly.

• The existing graphical confirmation plan is powerless against shoulder surfing assaults. Consequently, in view of the PassPoints, we include utilizing one-time session passwords and distracters to build up our PassMatrix validation framework that is impervious to shoulder surfing assaults.

PassMatrix

PassMatrix's authentication consists of a registration phase and an authentication phase as described below:

Registration phase

At this stage, the client makes a record which contains a username and a secret word. The secret key comprises of just a single pass-square per picture for an arrangement of n pictures. The quantity of pictures (i.e., n) is chosen by the client in the wake of considering the exchange off amongst security and convenience of the framework [42]. The main motivation behind the username is to give the client a creative ability of having an individual record. The username can be discarded if PassMatrix is connected to confirmation frameworks like screen bolt. The client can either pick pictures from a gave list or transfer pictures from their gadget

https://dx.doi.org/10.22161/ijaers/nctet.2017.13 *ISSN: 2349-6495(P) | 2456-1908(O)*

as pass-pictures. At that point the client will pick a passsquare for each chose pass-picture from the framework, which was partitioned by the picture discretization module. The client rehashes this progression until the secret word is set.

Authentication phase

At this stage, the client utilizes his/her username, secret word and login markers to sign into PassMatrix. The accompanying depicts every one of the means in detail:

1) The client inputs his/her username which was made in the enlistment stage.

2) another marker included a letter and a number is made by the login pointer generator module. The pointer will be indicated when the client employments

6. MODULES:

- Client Side Module
- Server Side Module

MODULES DESCRIPTION:

Android (Client side using ECLIPSE)

User Register and Logins using 3 modules

- MultiImage registration and Login
    - User is given by 3 images by default he has to touch and register and also logins by using the same.
- Image Login
    - Here only one image is given by default and it should be used for graphic authentication
- Color Login
    - User can touch any point on the image to get the color and register him with that color code and also logins using the same.

PHP (Server side using XAMPP)

- Here admin acts as a authority to approve the bill and also can view user details.
- Attacks are performed by users those attacks are viewed by admin as RANDOM ATTACKS

7. CONCLUSION

With the expanding pattern of web administrations and applications, clients can get to these applications whenever and anyplace with different gadgets. Keeping in mind the end goal to secure clients' advanced property, validation is required each time they attempt to get to their own record and information. Be that as it may, directing the verification prepare openly may bring about potential bear surfing assaults. Indeed, even a confused secret key can be broken effectively through shoulder surfing. Utilizing conventional printed passwords or PIN technique, clients need to sort their passwords to verify themselves and therefore these passwords can be uncovered effortlessly on the off chance that somebody looks over shoulder or uses video recording gadgets, for example, cell telephones.

To beat this issue, we proposed a shouldersurfing safe validation framework in light of graphical passwords, named PassMatrix. Utilizing a one-time login pointer per picture, clients can bring up the area of their pass-square without straightforwardly clicking or touching it, which is an activity defenseless against shoulder surfing assaults. In view of the outline of the level and vertical bars that cover the whole pass-picture, it offers no piece of information for assailants to limit the secret key space regardless of the possibility that they have more than one login records of that record. Besides, we actualized a PassMatrix model on Android and completed client analyses to assess the memorability also, ease of use. The exploratory outcome demonstrated that clients can sign into the framework with a normal of 1:64 tries (Median=1), also, the Total Accuracy of all login trials is 93:33% even two weeks after enlistment. The aggregate time expended to sign into PassMatrix with a normal of 3:2 pass-pictures is between 31:31 and 37:11 seconds and is viewed as worthy by 83:33% of members in our client think about.

REFERENCES

[1] S. Sood, A. Sarje, and K. Singh, "Cryptanalysis of password authentication schemes: Current status and key issues," in Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on, Dec 2009, pp. 1–7.

[2] S. Gurav, L. Gawade, P. Rane, and N. Khochare, "Graphical password authentication: Cloud securing scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on, Jan 2014, pp. 479–483.

[13] J. Long and K. Mitnick, No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Elsevier Science,2011.

[14] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected,"

https://dx.doi.org/10.22161/ijaers/nctet.2017.13 *ISSN: 2349-6495(P) | 2456-1908(O)*

IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 6, pp. 716–727, June 2014.
[22] X. Bai, W. Gu, S. Chellappan, X. Wang, D. Xuan, and B. Ma, "Pas: predicate-based authentication services against powerful passive adversaries," in 2008 Annual Computer Security Applications Conference. IEEE, 2008, pp. 433–442.
[23] Z. Zheng, X. Liu, L. Yin, and Z. Liu, "A stroke-based textual password authentication scheme," in Education Technology and Computer Science, 2009. ETCS'09. First International Workshop on, vol. 3. IEEE, 2009, pp. 90–95.
[24] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using captcha in graphical password scheme," in 2010 24th IEEE International Conference on Advanced Information Networking and Applications. IEEE, 2010, pp. 760–767.
[25] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. Nicholson, J. Nicholson, and P. Olivier, "Multi-touch authentication on tabletops," in Proceedings of the 28th international conference on Human factors in computing systems. ACM, 2010, pp. 1093–1102.
[26] "Black hat: Google glass can steal your passcodes," https://www.technologyreview.com/s/529896/black- atgoogle-glass-can-steal-your-passcodes/.
[27] A. De Luca, M. Harbach, E. von Zezschwitz, M.-E. Maurer, B. E. Slawik, H. Hussmann, and M. Smith, "Now you see me, now you don't: Protecting smartphone authentication from shoulder surfers,"
[28] E. von Zezschwitz, A. De Luca, and H. Hussmann, "Honey, i shrunk the keys: Influences of mobile devices on password composition and authentication performance," in Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, ser. NordiCHI '14. New York, NY, USA: ACM, 2014, pp. 461–470.
[29] A. Bianchi, I. Oakley, V. Kostak s, and D. S. Kwon, "The phone lock: Audio and haptic shoulder-surfing resistant pin entry methods for mobile devices," in Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction, ser. TEI '11. New York, NY, USA: ACM, 2011, pp. 197–200.
[30] A. Bianchi, I. Oakley, and D. S. Kwon, "The secure haptic keypad: A tactile password system," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ser. CHI '10. New York, NY, USA: ACM, 2010, pp. 1089–1092.
[31] I. Oakley and A. Bianchi, "Multi-touch passwords for mobile device access," in Proceedings of the 2012 ACM Conference on Ubiquitous Computing, ser. UbiComp '12. New York, NY, USA: ACM, 2012, pp. 611–612.
[32] M. Martinez-Diaz, J. Fierrez, and J. Galbally, "The doodb graphical password database: Data analysis and benchmark results," Access, IEEE, vol. 1, pp. 596–605, 2013.
[36] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in Proceedings of the working conference on Advanced visual interfaces, ser. AVI '06. New York, NY, USA: ACM, 2006, pp. 177– 184.
[37] B. Laxton, K. Wang, and S. Savage, "Reconsidering physical key secrecy: Teleduplication via optical decoding," in Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008, pp. 469–478.
[38] X. Suo, Y. Zhu, and G. Owen, "Analysis and design of graphical password techniques," Advances in Visual Computing, pp. 741–749, 2006.
[39] A. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. Smith, "Smudge attacks on smartphone touch screens," in USENIX 4th Workshop on Offensive Technologies, 2010.
[40] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," Computer Security– ESORICS 2007, pp. 359–374, 2007.
[41] "Secure socket layer ssl," http://en.wikipedia.org/wiki/ Transportn Layern Security.
[42] L. Cranor and S. Garfinkel, Security and Usability. O'Reilly Media, Inc., 2005.
[43] "Google play," https://play.google.com/store/.
[44] "Android developer," http://developer.android.com/index.html.
[45] "Android version of distribution," http://developer.android. com/resources/dashboard/platform-versions.html.
[46] J. Thorpe and P. van Oorschot, "Human-seeded attacks and exploiting hot-spots in graphical passwords," in Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium. USENIX Association, 2007, p.