

To Survey Graphical Password Verification Method

Khushboo Shrivastava¹, Harish Sahu²

¹Assistance professor, Department of Computer Science & Engineering

²Assistant Professor, Department of Computer Technology, CIET, Raipur

Abstract -In this present time, authentication is the way of giving persons access to system object based on user's uniqueness. If the codes match, the process will be succeed and user will get the consent to access the system. Text based password scheme follows the guidelines such as at least 8 characters long, should combine upper-case and lower-case and digit. user have problem to remember their complicated password over time due to the limitation of human brain, user tend to forget about their password. User tend to use the same password for all type of account. So if one account is hacked, the possibility for other account to be hack is a high. Graphical password can be used as alternative to solve the issue related to the text-based authentication based on the fact that humans can tend to remember pictures batter then text. Now a day's many computer system, Network and internet based environment are trying to use of graphical authentication technique in this paper we make a survey of the basic authentication and its technique and also presents a comprehensive study of graphical password authentication method and graphical password system.

Keyword –Authentication, Comprehensive, Uniqueness, Survey

I. INTRODUCTION

A password authentication system allows user choice while influencing users toward stronger password identify that there are three major Areas where human computer interaction is important authentication, security operation and the developing secure system. Alphanumeric password where first presented in the 1960 as a result to security issues for first multiuser operating system. An alphanumeric password is only a sequence of letters and digits. Graphical password consist of choosing images or drawing symbol rather than entering textual character It was first described by Greg Blonder in 1996. Physiological studies have shown that people can remember pictures better than text human brain is capable of processing and storing large volume of graphical information with easiness...while it is very tough to recall a string of

fifty characters, humans are capable easy to recall faces of people places we visited and things.

A. Graphical Password Authentication Methods

1. Token based authentication method
2. Biometric based authentication method
3. Knowledge based authentication method

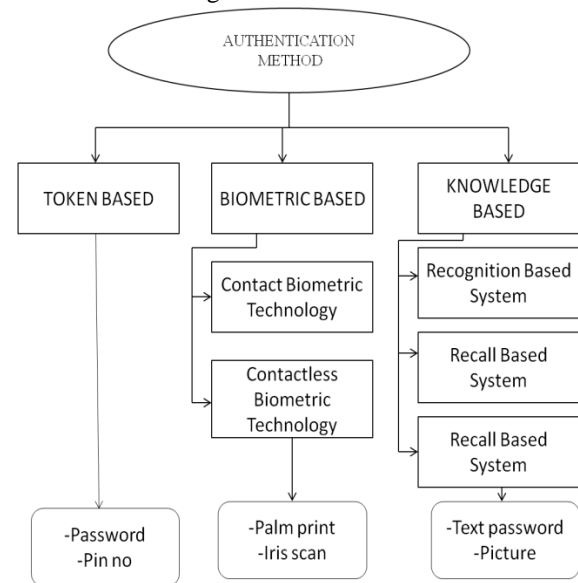


Figure1: Types of Authentication

1) Token based authentication: Token based techniques, like key cards, bank cards and smart cards are mostly used. Token based authentication systems also use knowledge-based techniques to upgrade security, for example: ATM cards are generally used together with a PIN number.

2) Biometric based authentication: Biometric based authentication techniques, such as a fingerprints, iris scan, or facial recognition, are not yet broadly accepted. the main drawback of this scheme is that such systems can be costly, and the identification system can be slow and often unreliable. However, This type of technique provide the uppermost level of security.

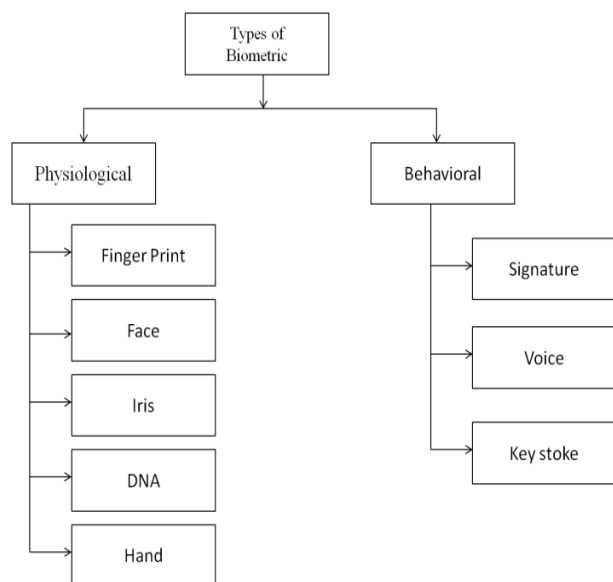


Figure 2: Types of Biometric Authentication

3) Knowledge Based Authentication: knowledge based authentication method are the further most broadly used authentication techniques and include both text-based and picture-based password the picture based techniques can be further divided into two system:-recognition based authentication system and recall based the graphical authentication system knowledge based authentication method shared secret key which is used in banks, financial institutions, internet service provider and email services provider like Gmail, Yahoo mail etc.

3.1) *Recognition based technique*: Dhamija and Perring advised a graphical authentication technique established on the Hash visualization scheme in their method the user is asked to select a certain number of pictures from a set of random images generated by a program later the user will be required to identify the preselected images in order to be authenticated. A

weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain tab text.

3.2) *Recall based techniques*: In the recall based techniques user need to recall or remember the particular images or drawing which he or she has already generated in the phase of registration. There are lots of techniques provided for recall based scheme. Here we have selected a scheme proposed by Jemyn called Draw-A- Secret (DAS) for our analysis. in this scheme user need to design a picture or signature on a 2D grid. The coordinate occupied by the picture drawn by user are stored in the order of drawing. In the authentication process user need to redraw the same picture. If the picture touches the same grid, then the user is authenticated.

II LITERATURE REVIEW

These including a few article and journal that related directly and indirectly to the secure graphical password system and also describe about the related research that is review for graphical password authentication which are being proposed. All this survey was described, summarized, evaluated and clarified.

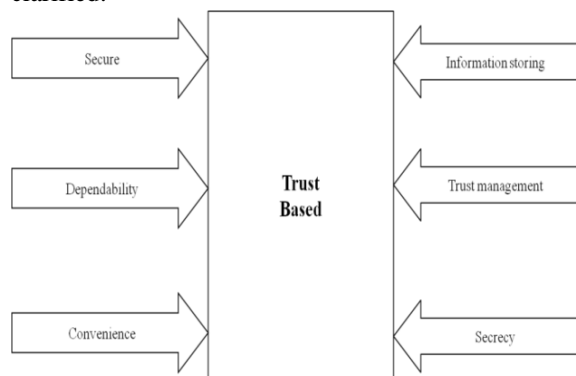


Figure 3: Authentication Based method

| S.No | Proposal/Author | Year | Objective | Trust | Accuracy | Techniques |
|------|--------------------|------|--|-------|----------|-----------------------------|
| 1 | G.E. Blonder | 1996 | Single image based schemes | ✓ | ✓ | Graphical password schemes |
| 2 | Greg. E. Blonder | 1996 | Database consist of predefined images which will be displayed to the user has to top region of interest as to set the password | ✓ | ✓ | Cued recall based technique |
| 3 | Brostoff | 2000 | User have to chose four faces as a password from 3×3 matrix[Passface Scheme] | ✓ | ✓ | Recognition based technique |
| 4 | Dhamiya and Perrig | 2000 | Users have to choose a random image from a set of images | ✓ | ✓ | Recognition based technique |

| | | | | | | |
|----|---|------|---|---|---|---|
| 5 | Jensen | 2003 | User has to select image of size 40×40 from a 5×5 matrix[Picture Password Scheme] | ✓ | ✓ | Recognition based technique |
| 6 | Tharpe and vanoorschot | 2004 | Allow user to create free-hand drawing as a password | ✓ | ✓ | Pre recall based technique[Graphical Password Scheme] |
| 7 | Varenhorst | 2004 | Allow user to create free-hand drawing as a password | ✓ | ✓ | Pre recall based technique[Passdoodle] |
| 8 | G.E. Blonder | 2005 | By Eliminating the pre define boundaries and allowing arbitrary images | ✓ | ✓ | Passpoint Method |
| 9 | Sobardo and Birget | 2006 | User chooses these pass-object and click inside of a convex formed by the pass objects | ✓ | ✓ | Recognition based technique[Shoulder Surfing Problem] |
| 10 | BDAS | 2007 | User's choice depends on various characteristics of image | ✓ | ✓ | Cued recall based technique |
| 11 | Chiasson[Cued Click Points] | 2007 | Location of the click point of the current image the next image is displayed | ✓ | ✓ | Cued recall based technique |
| 12 | Chissaon | 2007 | Includes persuasive features to cued click point | ✓ | ✓ | Cued recall based technique |
| 13 | Thao and Li | 2007 | It provide features of both textual as well as Graphical Password | ✓ | ✓ | Hybrid based technique |
| 14 | Jermyn | 2009 | User have to draw a password on a 2D grid using stylus or mouse | ✓ | ✓ | Pre recall based technique[“Draw-A-Secret”][DAS] |
| 15 | Samaneh Farmand[Syakri Algorithm] | 2009 | User is authenticated by drawing their signature with the help of a mouse of stylus | ✓ | ✓ | Pre recall based technique |
| 16 | Jiminy | 2011 | User are provided an image as a reminder to choose Graphical Password that are easy to remember | ✓ | ✓ | Hybrid based technique |
| 17 | H. Gao [Uses CAPTCHA => Completed automated public training Turning test to tell computer and humans apart] | 2011 | Provides features of both Graphical Password scheme as well as CAPTCHA technology | ✓ | ✓ | Hybrid based technique |
| 18 | H. Gao | 2011 | Passhands is a combination of Recognition based and Palm based Biometric technique | ✓ | ✓ | Hybrid based technique |
| 19 | Shraddha M.Gurav, Leena S.Gawade | 2014 | Graphical Password Authentication | ✓ | ✓ | Cloud Securing Scheme |
| 20 | Weiss | 2015 | Geometric Shapes are generated on basis of the combination of eight strokes | ✓ | ✓ | Pre recall based technique[Pass shapes] |
| 21 | Harsh Desai,Ninaad Suvarna | 2015 | Grid Based Authentication Password | ✓ | ✓ | Hash Technique |
| 22 | Abhilash M Joshi, Balachandra Muniyal | 2018 | On selection of strict sequence of the image,a two digit number is shown | ✓ | ✓ | Authentication using text and Graphical Password |
| 23 | Altaf Khan, Dr.Alexander G. Chefranov | 2020 | A captcha-based graphical password with strong password space and usability study | ✓ | ✓ | Captcha-Based Password Scheme |
| 24 | Istanbul,Turkey | 2020 | Graphical password with strong password space and usability stude | ✓ | ✓ | CAPTCHA-Based Technique |
| 25 | Jouraj khadadadi, Yashar Javadianasl Farnak Rabiei, M.Alizadeh | 2021 | A novel graphical password authentication Scheme with improved usability | ✓ | ✓ | Recognition-based graphical password |

III CONCLUSION

In this survey, I have focused an comprehensive study of current Graphical Password Techniques, Different techniques from recognition based, Cued recall based and Hybrid schemes of Graphical Password Techniques are observed and reviewed. Though the main consultation for graphical based password is that people are better at remembering picture password than text based passwords, our fundamental analysis proposes that it is very complicated to break graphical password using various method. Therefore, it can be concluded that, we need our authentication system to be more reliable robust and Secure as there is always a place for improvement.

My primary analysis justify that it is harder to break graphical password using the traditional attack approaches such as brute force search, dictionary attack or spyware. much more research and user studies are needed for graphical password technique to reach higher levels of capability and cooperation.

REFERENCE

- [1] Dec 2009, H. Gao proposed paper on “graphical password scheme using color login”.
- [2] In May 2011, M. Sreelatha proposed Hybrid Textual Authentication Scheme.
- [3] Er. Aman Kumar, Er. Naveen Bilandi, Department of Computer Science and Engineering, DAV University, Jalandhar, Punjab, India “Graphical Password Based Authentication Based System for Mobile Systems”.
- [4] Miss.Swati Tidke, Miss Nagama Khan, Miss.Swati Balpande Computer Engineering, RTM nagpur university, M.I.E.T Bhandara, “Password Authentication Using Text and Colors”.
- [5] Veena Rathanavel, Swati Mali, Student M. Tech, Department of Computer Engineering, K J Somaiya, College of Engineering Mumbai, “Graphical Password as an OTP”.
- [6] Veena Rathanavel, Swati Mali, Student M. Tech, Department of Computer Engineering, K J Somaiya, College of Engineering Mumbai, “Graphical Password as an OTP”.
- [7] In 2017 Aayush Dilipkumar Jain, Ramkrishna Khetan Krishnakant Dubey, Prof. Harshali Rambade K. Elissa, Department of Information Technology Vidyalkar Institute of Technology, Mumbai, “Color Shuffling Password Based Authentication”.
- [8] Harsh Kumar Sarohi, Farhat Ullah Khan, “Graphical Password Authentication Schemes: Current Status and Current Issues,” IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 1, March 2013.
- [9] “Graphical Passwords: A Survey” by Xiaoyuan Suo, Ying Zhu, G. Scott. Owen.
- [10] R. Dhamija and A. Perrig, “Déjà vu: A User Study Using Images for Authentication”, In Proceedings of the USENIX Security Symposium, 2000.
- [11] I. Jermyn, A. Mayer, F. Monrose. M. K. Reiter and A. D. Rubin, “The Design and Analysis of Graphical Passwords”, In Proceedings of the 8th USENIX Security Symposium, 1999.
- [12] G. Blonder, “Graphical Password”, In Lucent Technologies, Inc., Murray Hill, NJ, United States Patent 5559961, 1996.
- [13] Passlogix <http://www.passlogix.com>, Accessed on February 2007. [11] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, “Authentication Using Graphical Passwords: Basic Results”, In Human-Computer Interaction International (HCII 2005), Las Vegas, NV, 2005.
- [14] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.
- [15] Real User Corporation, Passfaces TM <http://www.realuser.com>, Accessed on January 2007.
- [16] R. Dhamija, and A. Perrig, “Déjà vu: A User study Using Images for Authentication”, in 9th Unisec Security Symposium, 2000.
- [17] Scheier, Bruce, “Cryptanalysis of MD5 and SHA: Time for a New Standard”, Computerworld, retrieved 15 October 2014.
- [18] A. Almulhem, “A graphical password authentication system,” in internet security (World CIS), 2011 World Congress on, pp. 223-225, IEEE, 2011.
- [19] X. Suo, Y. Zhu, and G. S. Owen, “Graphical password; A survey,” in computer security application conference, 21st annual, pp, 10-pp, IEEE, 2005.

- [20] O.Ayannuga,Olanrewaju and F. Olusegun, "Graphic-text Authentication of a window-based application," International journal of computer application,vol.21,no.6,pp.36-42,2011.
- [21] M.G. Tuscano and A. Tulasyan,"Graphical Password Authentication using pass faces," International journal of engineering research and application,vol.5.no.3,pp.60-64,2015.
- [22] H. yuan, Y. Han, and j. Hu, "password memorability and security empirical results," Int. Comput Sci. Softw. Eng. Conf. Vol. 4,pp.25-3,2008.
- [23] D.R. Pilar,A. Jaeger,C.F.A.Gomes, and L.M.Stein,"Passwords usage and Human memory limitations: a survey across age and educational background," PLoS One, vol 7,no. 12,2012.
- [24] P.Elftmann,"Secure alternatives to authentication mechanisms submitted by," Aachen Univ.Aachen,Gen.Thesis,October 2006,pp.1-92.
- [25] S.Chiasson, P.C.van.Oorschot, and R.Biddle," Graphical Password authentication using Cued click point,"pp.359-374,2007.