International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Two Way Text and Pixel Based Authentication

Dr Padmanjali.A.Hagargi, Nishath Humaira, Nisha ,Iqra Tanzeem,Angelen Elizabeth

Dept Of CSE ,GNDEC, Bidar /585403, India

ABSTRACT

Text passwords and personal identification numbers (PINs) are a great way to verify authenticity, as they are simple and can be used in programs that include social terminals, the web, and mobile devices. suggest graphical word processing programs based on input such as selecting image components. These programs have been shown to improve memory without sacrificing installation time or error rates while also maintaining high resistance to high power and predictor attacks However, click-through passwords reveal their own problems. Another issue is their involvement in clever guesses and shoulder attacks. Such attacks are effective because the parts of the image that users choose as password items are both easy for the attacker to view by taking a shoulder shot or setting the camera to record input and also predictable - users tend to choose the most aggressive places like eyes and face. This problem is a big problem as the graphical content of the graphical password system is often stored on authentication servers and easily presented to attackers in response to easily accessible identity information. To address this issue, we are introducing a new point-to-point click-through program, PassBYOP-Submit your image, which increases resistance to view attacks by combining a user's password on an image or physical object.

1. Introduction

passwords suffer from limitations in terms of memorability and security—passwords that are difficult to guess are also hard to remember In order to mitigate these problems, researchers have proposed graphical password schemes that rely on input such as selecting portions of an image. These systems have been shown to improve memorability without sacrificing input time or error rates while also maintaining a high resistance to brute force and guessing attacks However, graphical passwords present their own problems. One issue is their susceptibility to intelligent guessing and shoulder-surfing attacks. Such attacks are effective because the sections of images that users select as password items are both easy for an attacker to observe by snooping over shoulders or setting up a camera to record input and also relatively predictable—users tend to choose hotspots such as the eyes in a facial portrait. This issue is particularly problematic as the image contents for graphical password systems are typically stored on authentication servers and readily presented to attackers in response to input of easily accessible user identity information. To address this issue, we present a new point-click graphical password system, PassBYOP—Bring Your Own Picture, that increases resistance to observation attack by coupling the user's password to an image or object physically possessed.

2. Literaturesurvey

- Shraddha D. Ghogare, Swati P. Jadhav, Ankita R. Chadha, Hima C. Patil, "Location Based Authentication: A New Approach towards Providing Security", International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012
- M. Bishop, S.S. Venkatramanayya, "Introduction to Computer Security", Pearson Education, 2009

3. SystemSpecification

3.1 SystemRequirements

Entire work will be executed in Eclipse IDE which provides environtment to run Java Applications using Tomcat which is a web server to provide an environment to run an applicationand MySQL for Database.

- Eclipse
- Tomcat
- MySQL
- JDK
- JSP

4. ProblemDefinition

graphical passwords present their own problems. One issue is their susceptibility to intelligent guessing and shoulder-surfing attacks. Such attacks are effective because the sections of images that users select as password items are both easy for an attacker to observe by snooping over shoulders or setting up a camera to record input and also relatively predictable—users tend to choose hotspots such as the eyes in a facial portrait. This issue is particularly problematic as the image contents for graphical password systems are typically stored on authentication servers and readily presented to attackers in response to input of easily accessible user identity information

5. SystemDesign

Design for Web Apps encompasses technical and non-technical activities. The look and feel of content is developed as part of graphic design; the aesthetic layout of the user interface is created as part of interface design; and the technical structure of the WebApp is modeled as part of architectural and navigational design.

6. Scope Of TheProject

The purpose of this project We present a new point-click graphical password system, PassBYOP—Bring Your Own Picture, that increases resistance to observation attack by coupling the user'spassword to an image or object physically possessed. this paper proposed improving the security of graphical password systems by integrating live video of a physical token that a user carries with them. It first demonstrates the feasibility of the concept by building and testing a fully functional prototype. It then illustrates that user performance is equivalent to that attained in standard graphical password systems through a usability study assessing task time, error rate, and subjective workload.

7.Acknowledgements

I am highly intended my project guide **Dr Padmanjali.A.Hagargi**, for guiding and giving me timely advices and suggestions in successful completion of seminar work.

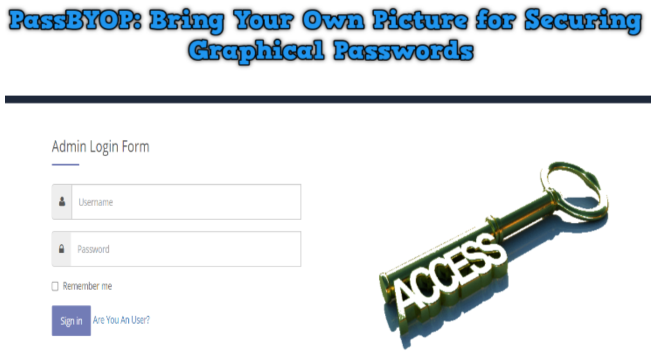
My sincere thanks to **Prof. Dayanand Jamkhandikar**HOD of Computer Science and Engineering department for his whole hearted support in completion of seminar.

I would like to express my deep sense of gratitude to principal **Ravindra Eklarkar**GURU NANAK DEV ENGINEERING COLLEGE, BIDAR for his motivation and for creating the inspiring atmosphere in the college providing state of art facilities for preparation and delivery of project. Finally, I thank all the staff members who directly or indirectly helped me to complete this project.

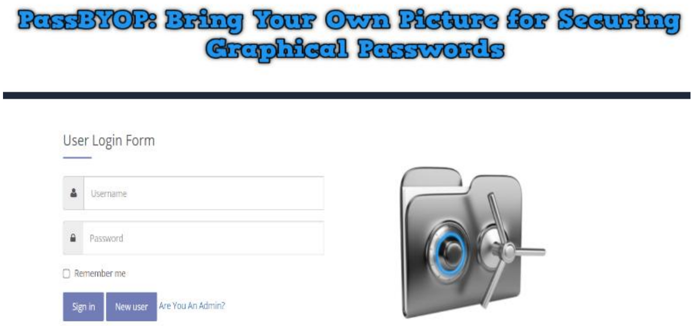
8. Methodology

- User Registration
- Upload Image
- Hash Code Generation and GLCM Process
- User Login Process
- Admin

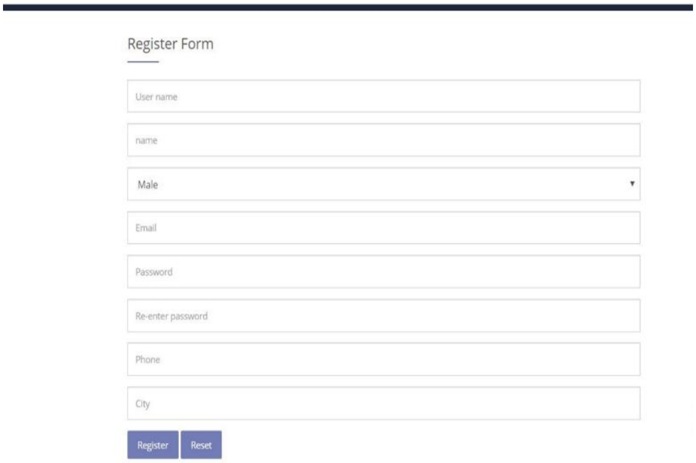
9. Expectedoutcome


PassBYOP: Bring Your Own Picture for Securing Graphical Passwords

Admin Login Form


PassBYOP: Bring Your Own Picture for Securing Graphical Passwords

User Login Form



Register Form

User name

name

Male

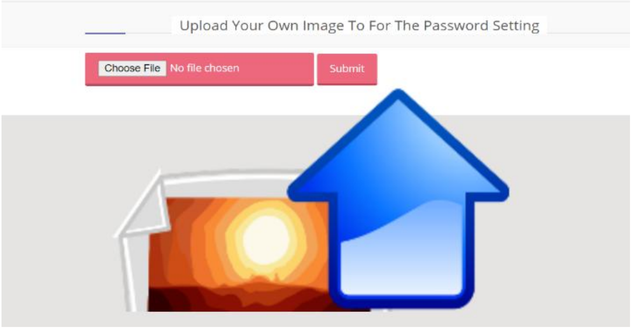
Email

Password

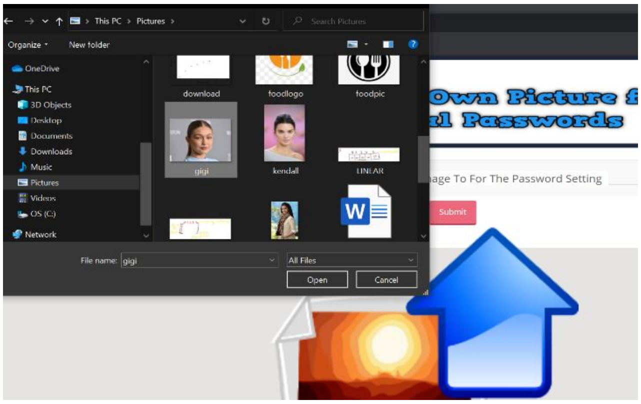
Re-enter password

Phone

City



Upload Your Own Image To For The Password Setting



File name: gigi

All Files

References

[1] M. Bishop, S.S. Venkatramanayya, “Introduction to Computer Security”, Pearson Education, 2009

[2] Shraddha D. Ghogare, Swati P. Jadhav, Ankita R. Chadha, Hima C. Patil, “Location Based Authentication: A New Approach towards Providing Security”, International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012. ISSN 2250-3153 International Journal of Computer Applications (0975 – 8887) International Conference on Communication Technology 2013 4

[3] Sharma, Seema, "Location Based Authentication" (2005). University of New Orleans Theses and Dissertations. Paper 141. [Online]. Available: http://scholarworks.uno.edu/cgi/viewcontent.cgi?article=1145&context=td

[4] J. Brainard, A. Juels, R. Rivest, M. Szydlo, M. Yung, “Fourth Factor Authentication: Somebody you know”, ACM’06. [Online]. Available: http://www.rsasecurity.ca/rsalabs/staff/bios/ajuels/publications/fourth-factor/ccs084-juels.pdf

[5] (2013) Imperva Site [Online]. Available: http://www.imperva.com/docs/wp_consumer_password_worst_practices.pdf

[6] M. Whitman, H. Matt ford, “ Principles of Information Security”,2 Nd Ed. Cengage Learning,2009

[7] I. Rock and P. Engelstein, “A study of Memory for Visual Form”,[Online]. Available: http://www.jstor.org/stable/1419366

[8] L. Standing,” Learning 10,000 Pictures”,[online]. Available: http://cvcl.mit.edu/SUNSeminar/standing73.pdf

[9] G. Danezis and A. Serjantov, “ Statistical Disclosure or Intersection attacks on anonymity systems”,[Online]. Available: http://research.microsoft.com/enus/um/people/gdane/papers/poolsda3.pdf