

International Journal of
Engineering Research and Science & Technology



ISSN : 2319-5991

www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

WEB BASED GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

Maltesh Kamatar, Amruthavarshini. A.S, Naveen Kumar. H

Asst. Professor, Asst. Professor, Asst. Professor

maltkpl@gmail.com, amruthavarshini233@gmail.com, navee2312@gmail.com

Department of CSE, Proudhadavaraya Institute of Technology, Abheraj Baldota Rd, Indiranagar,
Hosapete, Karnataka-583225

ABSTRACT:

As an alternative to the more commonplace alphanumeric passwords, graphical passwords show promise. People are more likely to recall visuals than words, which is why they are appealing. Our proposed graphical password authentication method is brief and to the point in this expanded abstract. Using a few examples, we outline how it works and draw attention to key features of the system.

Keywords: Password, graphical, high security

I.INTRODUCTION

User authentication is a fundamental component in most computer security contexts. It provides the basis for access control and user accountability [1]. While there are various types of user authentication systems, alphanumeric username/passwords are the most common type of user authentication. They are versatile and easy to implement and use.

Alphanumeric passwords are required to satisfy two contradictory requirements. They have to be easily remembered by a

user, while they have to be hard to guess by impostor [2]. Users are known to choose easily guessable and/or short text passwords, which are an easy target of dictionary and brute-forced attacks [3, 4, 5]. Enforcing a strong password policy sometimes leads to an opposite effect, as a user may resort to write his or her difficult-to-remember passwords on sticky notes exposing them to direct theft.

In the literature, several techniques have been proposed to reduce the limitations of alphanumeric password. One proposed

solution is to use an easy to remember long phrases (passphrase) rather than a single word [6]. Another proposed solution is to use graphical passwords, in which graphics (images) are used instead of alphanumerical passwords [7]. This can be achieved by asking the user to select regions from an image rather than typing characters as in alphanumeric password approaches.

In this extended abstract, we propose a graphical password authentication system. The system combines graphical and text-based passwords trying to achieve the best of both worlds. In section 2, we provide a brief review of graphical passwords. Then, the proposed system is described in section 3. In section 4, we briefly discuss implementation and highlight some aspects about the proposed system.

II. EXISTING SYSTEM:

Graphical passwords refer to using pictures (also drawings) as passwords. In theory, graphical passwords are easier to

remember, since humans remember pictures better than words [8]. Also, they should be more resistant to brute force attacks, since the search space is practically infinite. In general, graphical passwords techniques are classified into two main categories: recognition-based and recall based graphical techniques [7]. In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Passfaces is a recognition-based technique, where a user is authenticated by challenging him/her into recognizing human faces [9]. An early recall-based graphical password approach was introduced by Greg Blonder in 1996 [10]. In this approach, a user create a password by clicking on several locations on an image. During authentication, the user must click on those locations. PassPoints builds on Blonders idea, and overcomes

some of the limitations of his scheme [2]. Several other approaches have been surveyed in the following paper [7].

III. PROPOSED SYSTEM:

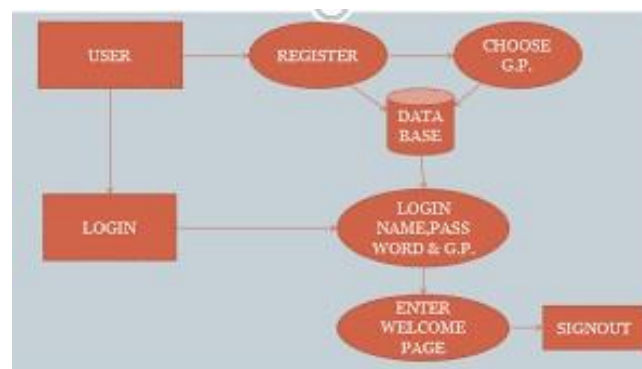
The proposed authentication system works as follows. At the time of registration, a user creates a graphical password by first entering a picture he or she chooses. The user then chooses several point-of-interest (POI) regions in the picture. Each POI is described by a circle (center and radius). For every POI, the user types a word or phrase that would be associated with that POI. If the user does not type any text after selecting a POI, then that POI is associated with an empty string. The user can choose either to enforce the order of selecting POIs (stronger password), or to make the order insignificant. The user can choose either to enforce the order of selecting POIs (stronger password), or to make the order insignificant.

In Figure 1, we show an example of a user creating a graphical password. In this example, the user chooses a picture of his or her kids by pressing “Load Image

button”. Then the user clicks on the kids faces in the order of their ages (order is enforced). For each selected region, the user types the kid’s name or nickname.



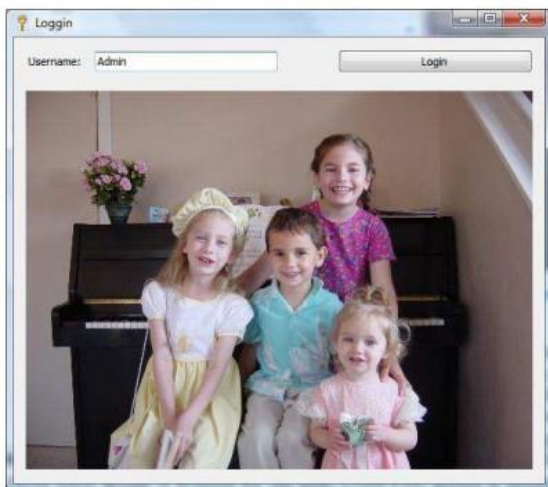
For authentication, the user first enters his or her username. The system, then, displays the registered picture. The user, then, has to correctly pick the POIs and type the associated words. At any time, typed words are either shown as asterisks (*) or hidden. In Figure, we show an example of the login screen.



IV. METHODOLOGY

The proposed system was implemented using Visual Basic .net 2005 (VB.net). The implementation has three main classes:

- Login Info: Contains username, graphical password, and related methods.
- Graphical Password: Contains graphical password information and related methods.
- Sel Reg: Contains fields about selected regions (POIs).

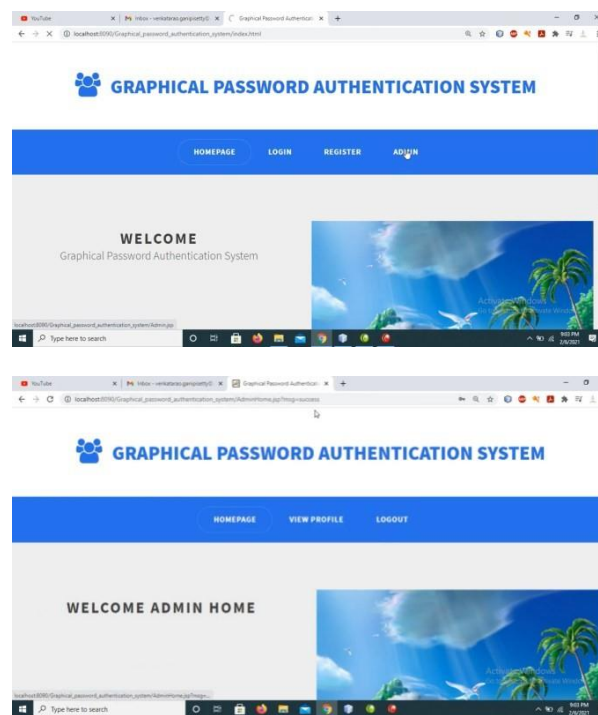


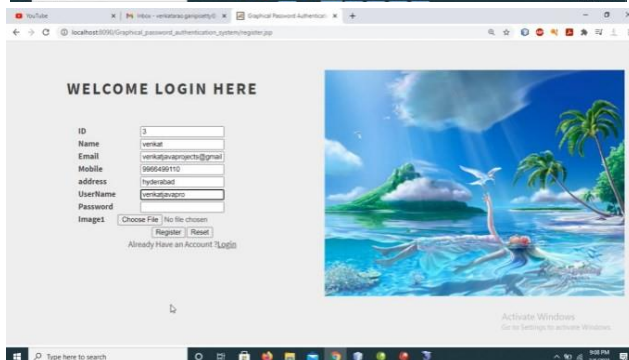
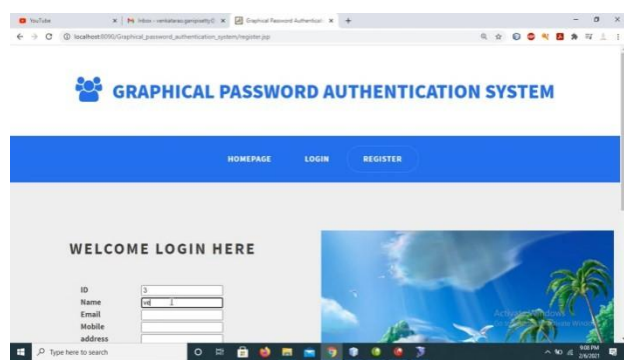
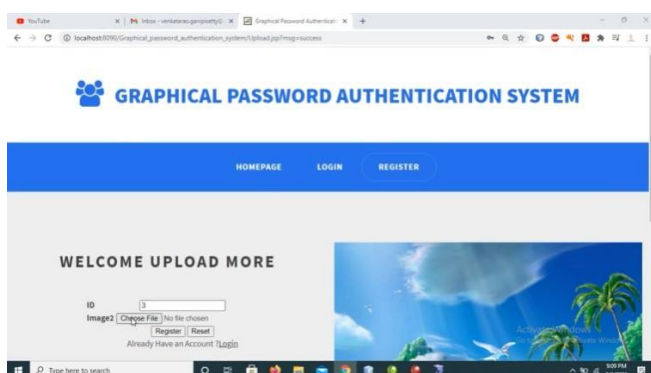
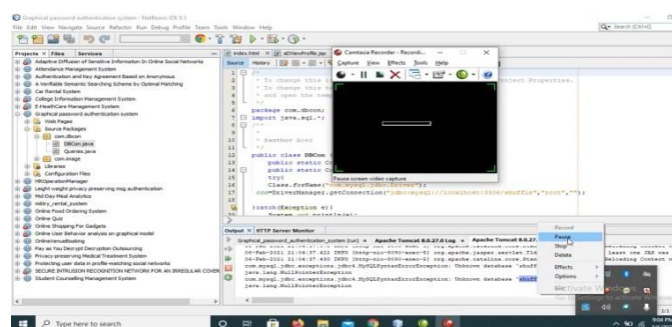
In the proposed system, a user freely chooses a picture, POIs and corresponding words. The order and number of POIs can

be enforced for stronger authentication. Together, these parameters allow for a very large password space. We believe that proposed approach is promising and unique for at least two reasons

- It combines graphical and text-based passwords trying to achieve the best of both worlds.
- It provides multi-factor authentication (graphical, text, POI-order, POI-number) in a friendly intuitive system.

V. OPERATION:





VI. CONCLUSION

For the vast majority of computer security scenarios, user

authentication is an essential component. We presented a basic graphical password authentication mechanism in this expanded abstract. In an effort to provide the greatest of both worlds, the system integrates both visual and text-based passwords. Additionally, it offers a user-friendly and straightforward system with multi-factor authentication. Using a few examples, we outlined how the system works and emphasised its key features.

VII. REFERENCES

[1] William Stallings and Lawrie Brown. *Computer Security: Principle and Practices*. Pearson Education, 2008.

[2] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Passpoints: design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, 63:102–127, July 2005.

[3] Robert Morris and Ken Thompson. Password security: a case history.

Communications of the ACM, 22:594–597, November 1979.

[4] Daniel V. Klein. Foiling the Cracker: A Survey of, and Improvements to, Password Security. In *Proceedings of the 2nd USENIX UNIX Security Workshop*, 1990.

[5] Eugene H. Spafford. Observing reusable password choices. In *Proceedings of the 3rd Security Symposium*. Usenix, pages 299–312, 1992.

[6] Sigmund N. Porter. A password extension for improved human factors. *Computers & Security*, 1(1):54 – 56, 1982.

[7] Xiaoyuan Suo, Ying Zhu, and G. Scott Owen. Graphical passwords: A survey. In *Proceedings of Annual Computer Security Applications Conference*, pages 463–472, 2005.

[8] Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems.

International Journal of Human-Computer Studies, 63:128–152, July 2005.

[9] Real User Corporation. The science behind passfaces, June 2004.

[10] G. E. Blonder. Graphical password. U.S. Patent 5559961, Lucent Technologies, Inc. (Murray Hill, NJ), August 1995.