Journal of Analysis and Computation (JAC)
(An International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861
Volume XVII, Issue II, July-Dec 2023

A Graphical Password Authentication System

Sparsh Mittal[1], Shyam Garg[2], Dr S K Singh[3]

[1]B.Tech Student, Department of Information Technology, JECRC College
[2]B.Tech Student, Department of Information Technology, JECRC College
[3]Profesoor, Department of Information Technology, JECRC College

ABSTRACT

Graphic passwords are a powerful alternative to traditional alphanumeric passwords. They are attractive because people usually remember pictures better than words. This high-level summary proposes a simple graphical password authentication system. We will use some examples to explain how it works and highlight important aspects of the system.

Index Terms - Security, scalability, passwords interoperability

[1] INTRODUCTION

User authentication is a fundamental component in most computer security contexts. It provides the basis for access control and user accountability [1]. There are many types of user authentication systems, but the alphanumeric username/password is the most common type of user authentication. They are versatile and easy to implement and use. Two conflicting requirements require an alphanumeric password. It should be easy for users to remember and hard for scammers to guess. Users are known to choose easy-to-guess and short text passwords. These are easy targets for dictionary and brute force attacks . Enforcing a strict password policy can have the opposite effect. Because the user could write her hard-to-remember password on a sticky note, exposing it to outright theft. The literature suggests several techniques for reducing the restrictions on alphanumeric passwords. One solution proposed by is to use a long, easy-to-remember phrase (passphrase) instead of a single word. Another proposed solution is to use graphical passwords where graphics (pictures) are used instead of alphanumeric passwords. This can be achieved by prompting the user to select her region from the image rather than entering the characters, like her alphanumeric password approach. This high-level abstract proposes a graphical password authentication system. This system combines graphical and text-based passwords to give you the best of both worlds. Section 2 provides a brief introduction to graphical passwords. Then, the proposed system is de-scribed in section 3.

In section 4, we briefly discuss imple-mentation and highlight some aspects about the proposed system. As the name suggests, it uses different types of shapes and images as password. In addition, scientist is saying that it's easy to remembered a picture for human brain than text. The human brain can easily process images. And image base password, it is resistant of dictionary attack, keylogger, social engineering.

Graphical passwords refer to using images (including drawings) as passwords. In theory, people remember pictures better than words, so graphical passwords are easier to remember [8]. Brute he should also be more resilient to Force attacks, as the search space is effectively infinite. In general, graphical password techniques fall into his two main categories: recognition-based and memory-based graphical techniques [7]. Recognition-based technology authenticates the user by prompting them to identify one or more images of her that they have chosen during the enrollment phase. In memory-based techniques, users are asked to reproduce previous creations or selections during the registration phase. Passfaces is a recognition-based technology that authenticates users by having them recognize human faces [9]. An early memory-based graphical his password approach was introduced by Greg Blonder in 1996 [10]. With this approach, the user creates a password by clicking multiple places on the image. The user must click these locations during authentication. PassPoints builds on Blonder's ideas and overcomes some of the limitations of his scheme [2]. In the next study, several other approaches were considered [7].

[2] PROPOSED WORK

The proposed authentication system works as follows. During registration, the user creates a graphic her password by entering the first selected image. The user then selects multiple point-of-interest (POI) regions in the image. Each POI is represented by a circle (center and radius). For each POI, the user enters a word or phrase associated with that POI for her. If the user does not enter any text after selecting a POI, the POI will be concatenated with an empty string. Users can enforce POI selection order (stronger passwords) or ignore the order. Figure 1 shows an example of a user creating his password graphically. In this example, the user clicks the Load Image button and selects an image of the child. The user then clicks on the children's faces in order of age (the order is enforced). For each region selected, the user enters the child's name or nickname. User has to authenticated by choosing one pr more images which he chooses during the registration time. In recall-based techniques is a process that user has to remember that was done during registration time.

Figure 1. An example of creating a graphical password using the proposed system

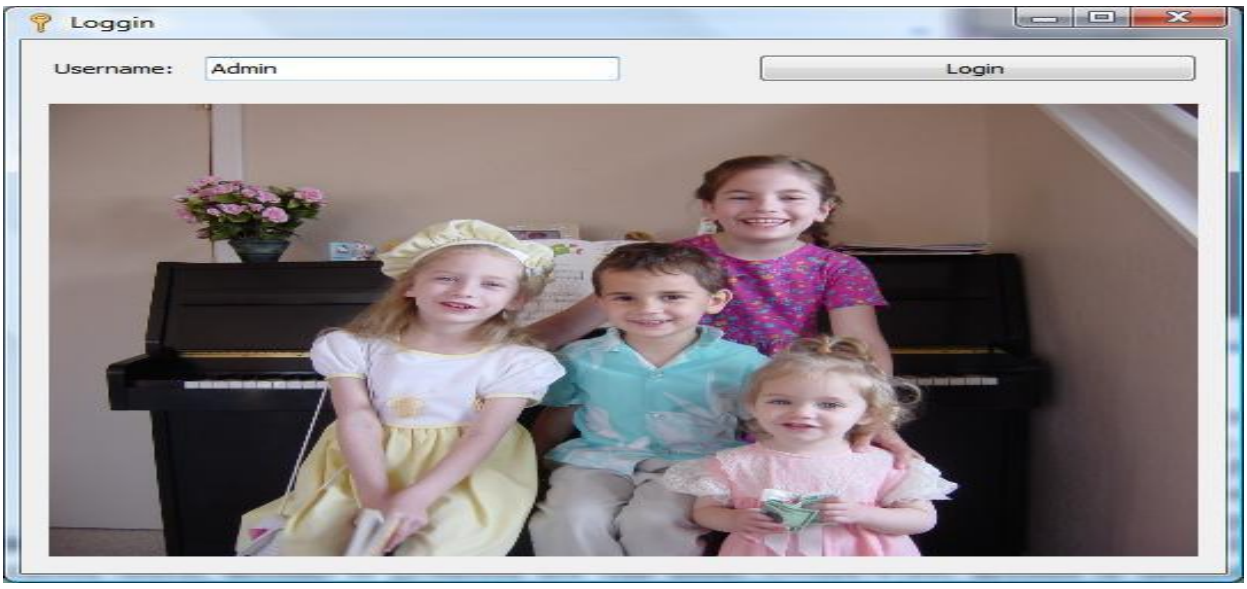
For authentication, users first enter their username. The registered image is displayed. The user then has to correctly select her POI and enter the associated word. Words you type appear as asterisks (*) or are hidden at any time. Figure 2 shows an example login screen.

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

LoginInfo: Contains username, graphical password, and related methods.

GraphicalPassword: Contains graphical password in-formation and related methods.

SelReg: Contains fields about selected regions (POIs).



In the proposed system, users freely select images, POIs, and corresponding words. For stronger authentication, you can enforce the order and number of POIs. Combining these parameters allows for a very large password space. We believe the proposed approach is promising and

unique for at least two reasons. A user-friendly and intuitive system that offers multi-factor authentication (graphic, text, POIorder,POInumber).

3. CONCLUSION

User authentication is a fundamental component in most computer security contexts. In this high-level summary, we proposed a simple graphical password authentication system. This system combines graphical and text-based passwords to give you the best of both worlds. It also offers multi-factor authentication with a user-friendly and intuitive system. Several examples were used to illustrate system operation and highlight important aspects of the system. Digital devices are becoming part of our lives. Using a digital device made me aware of the authentication process. Validation is an integral part of security. Authentication enhances customer security. Certain review articles explore the same areas for specific attacks found during testing. Hidden term print authentication is an excellent test device. It's more convenient and secure compared to the old old graphical password authentication system. A very large password space provides security against brute force attacks. Usage is simple. Passwords are easy to create and retrieve. Randomization in both authentication systems provides strong security against shoulder surfing. A good system requires high security and ease of use, and they are inseparable. Shoulder navigation attacks are subject to safeguards. However, the proposed method for the shoulder surfing problem still needs to be improved. This system can also be used to add a high level of security to text-based password systems.

4. REFERENCES

[1].William Stallings and Lawrie Brown. Computer Se-curity: 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 Sympo-sium. Usenix, pages 299–312, 1992.

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

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

[8] Antonella De Angeli, Lynne Coventry, Graham John-son, and Karen Renaud. Is a picture really worth a thousand words? exploring the feasibility of graphi-cal 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.